

Tilburg University

Het risico van de mobiele burger

van Ooijen, C.W.

Publication date:
2014

Document Version
Publisher's PDF, also known as Version of record

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
van Ooijen, C. W. (2014). *Het risico van de mobiele burger: Publieke mobiliteitssurveillance voor informatie over het gaan en staan van burgers.* [, Tilburg University]. Boom Lemma uitgevers.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Het risico van de mobiele burger

Omslagontwerp: Haagsblauw, Den Haag

Illustratie omslag: Brigitte van Ooijen (2014). *Eye on movement*. Acrylinkt op papier.

© 2014 Charlotte van Ooijen | Boom Lemma uitgevers

Behoudens de in of krachtens de Auteurswet gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprerecht (Postbus 3051, 2130 KB Hoofddorp, www.reprerecht.nl). Voor het overnemen van (een) gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (art. 16 Auteurswet) kan men zich wenden tot de Stichting PRO (Stichting Publicatie- en Reproductierechten Organisatie, Postbus 3060, 2130 KB Hoofddorp, www.stichting-pro.nl).

No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without written permission from the publisher.

ISBN 978-94-6236-478-3

ISBN 978-94-6274-170-6 (e-book)

NUR 805

www.boomlemma.nl

Het risico van de mobiele burger

Publieke mobiliteitssurveillance voor informatie over het gaan en staan van burgers

The risk of the mobile citizen

Public mobility surveillance for information about citizens' whereabouts
(with a summary in English)

Le risque du citoyen mobile

Surveillance publique de la mobilité du citoyen: où il est, où il va
(avec un résumé en Français)

Proefschrift

ter verkrijging van de graad van doctor
aan Tilburg University op gezag van de rector magnificus,
prof. dr. Ph. Eijlander, in het openbaar te verdedigen
ten overstaan van een door het college voor promoties
aangewezen commissie in de aula van de Universiteit
op vrijdag 17 oktober 2014 om 10.15 uur

door

Charlotte Willemijn van Ooijen

geboren op 5 november 1980 te Eindhoven

Promotiecommissie

Promotores: Prof. dr. P.H.A. Frissen
Prof. dr. P.J.A. De Hert

Overige leden: Prof. dr. V.J.J.M. Bekkers
Prof. dr. H.P.M. van Duivenboden
Prof. mr. J.E.J. Prins
Prof. dr. M. Thaens
Prof. mr. dr. S. Zouridis

*Voor mama,
mijn voortdurende inspiratie en bron van liefde*

VOORWOORD

Toen ik begon aan mijn promotietraject had ik het niet verwacht, maar tegelijkertijd verbaast het me ook niet van mezelf: ik schrijf mijn voorwoord in mijn nieuwe thuisstad Parijs. Mijn proefschrift rond ik af en daarmee een bewogen periode van mijn leven. Mijn weg naar dit moment en deze plaats heb ik niet van tevoren uitgestippeld, maar wel voor mogelijk gezien en in de loop der tijd met hulp van anderen gecreëerd en afgelegd. Mobiliteit is zowel in sociale als ruimtelijke zin beperkt te plannen, en gelukkig maar. Het leven zou te voorspelbaar worden en daarmee creativiteit en onverwacht geluk verhinderen. Ben ik dan niet blij mijn doel, een afgerond proefschrift, te hebben bereikt? Natuurlijk wel, maar het doet me evenveel deugd dat ik tijdens het traject hiernaartoe veel onvoorziene dingen heb meegemaakt. Een film van personen, plaatsen en momenten schiet door mijn hoofd. Inspirerende collegae, verrassende informanten, verbazingwekkende sprekers (niet altijd in positieve zin) en hartverwarmende vrienden en familieleden hebben mijn pad mede gevormd. Hier wil ik graag een aantal van hen danken voor hun bijdragen aan mijn denken, voelen en doen die hebben geleid tot de totstandkoming van dit boek en de weg ernaartoe waardevol hebben gemaakt.

Vanaf het begin van mijn promotietijd heb ik mij bewogen tussen twee vakgroepen die ooit één waren: het Tilburg Institute for Law, Technology, and Society (TILT) en de Tilburgse School voor Politiek en Bestuur (TSPB). Het was alsof ik werd geadopteerd door reeds gescheiden ouders die allebei al nieuwe gezinnen hadden gesticht. Het was even zoeken naar de juiste balans tussen mijn twee academische families. Aanvankelijk zag ik vooral mijn TILT-familie, omdat ik daar kost (wekelijkse vakgroeplunches) en inwoning (mijn vaste werkplek) kreeg. Mijn broeders en zusters van de TSPB zag ik de eerste tijd sporadisch, rondom een bezoek aan mijn promotor Paul Frissen, bij een lunch, bij DISCO, of tijdens het jaarlijkse familie-uitje naar EGPA. Tot mijn grote plezier werd de bezoekenregeling na anderhalf jaar uitgebreid. Vanaf september 2008 verbleef ik één dag per week bij TSPB in de functie van bestuurskundig docent, met ook daar een eigen werkplek. Zowel bij TILT als bij TSPB heb ik met veel plezier gewerkt. Ik dank de begeleiders, collegae en vrienden die ik bij beide vakgroepen heb gevonden.

Ik richt mij in het bijzonder tot mijn promotor Paul Frissen. Jouw stijl van begeleiden heb ik als uiterst prettig ervaren. Ik heb genoten van jouw liefde voor taal en oog voor de significante details in mijn teksten. Na een gesprek met jou ging ik veelal met nieuwe ideeën, vertrouwen en goede zin de deur uit. Ook was je er voor mij bij momenten van tegenslag en tragiek. Het is niet voor niets dat ik altijd met veel trots vertel dat jij mijn promotor bent.

Mijn tweede promotor, Paul De Hert, dank ik voor de steevast verrassende en vaak inspirerende reacties op mijn stukken evenals de vele nuttige literatuursuggesties. Ook heeft het mij veel plezier gedaan dat je de *francophone* in jou hebt aangesproken tijdens de laatste etappe van mijn proefschrift. In Colette Cuijpers heb ik de beste dagelijks begeleider gevonden die ik me maar kon wensen. Menig keer hebben we al genietend op een Bredaas terras gesproken over het proefschrift en andere zaken. Onze gesprekken waren en blijven zeer waardevol. Ook aan jouw inhoudelijke en redactionele commentaren op mijn teksten had ik heel veel, ondanks of misschien wel dankzij wat jij jouw lekenbril noemt. Sjaak Nouwt, jou dank ik voor de begeleiding tijdens mijn eerste schreden op het proefschriftpad, jouw blijvende interesse in mijn wel en wee na jouw vertrek bij TILT en voor het plezier van het samen schrijven van een publicatie. Miriam Lips, jij legde binnen het programma Ruimte voor Geo-informatie met het GeoGov-project de basis voor mijn promotie-onderzoek. Daarvoor ben ik je zeer erkentelijk.

Van TILT bedank ik verder mijn *roomie* Naveen Thayyil en Nadya Purtova voor de vele onvergetelijke momenten samen, en Corien Prins, Bert-Jaap Koops en Ronald Leenes voor verschillende inspirerende gedachtewisselingen. Mooie onderwijs-ervaringen, schrijfmomenten en menige festiviteiten heb ik onder meer gedeeld met enkele (oud-)collegae van de TSPB: Laurens de Graaf, Marcel Boogers, Martin Schulz, Meike Bokhorst, Niels Karsten, Rik Peeters, Stefan Soeparman en Ted van de Wijdeven. ¡Gracias, amigos y amigas! Speciale dank richt ik aan mijn paranimf Julien van Ostaaijen voor zijn vriendschap en het samen nuttigen van Belgische biertjes, dat daar doorgaans bij komt kijken. Collegiale steun vond ik het afgelopen jaar eveneens bij de Rotterdamse bestuurskundigen, waarvoor dank.

Dit proefschrift was niet tot stand gekomen zonder het benodigde veldonderzoek. Voor het kunnen verrichten van mijn eerste casestudy bij de ‘Politie Noodaalsstad’ zeg ik dank aan de leden van het Landelijk Programmabureau ANPR en aan mijn informanten van de ‘Politie Noodaalsstad’. Helaas kan ik jullie vanwege de afspraak tot anonimiseren niet bij naam bedanken. Van het Ministerie van Infrastructuur en Milieu bedank ik Gé van Toorenborg en Michiel Beck voor de introductie bij de Nationale Databank Wegverkeersgegevens (NDW), waar ik mijn tweede casestudy heb kunnen uitvoeren. Dank gaat ook uit naar de NDW-organisatie en alle betrokkenen bij het gevolgde aanbestedingstraject in het bijzonder.

Voor het laatste schaaft- en polijstwerk aan de tekst is een aantal mensen van onschatbare waarde geweest. Mariëlle van Delft, je hebt mij geweldig geholpen bij de laatste redactionele slag die ik moest slaan. Wie had dat gedacht toen we in de brugklas zaten? Naveen Thayyil, Vivian Carter en Diaswati Mardiasmo dank ik voor hun hulp bij mijn Engelse samenvatting. Voor het redigeren van mijn Franse samenvatting dank

ik mijn *équipe francophone*: Cécile Visini, Nicolas Mazeret, Robert Falce en Paul De Hert.

Van mijn familie en vrienden heb ik de nodige morele en praktische ondersteuning gekregen. Evelien, we zijn al bijna ons hele leven hartsvriendinnen en steunen elkaar door dik en dun. Jouw liefde en vertrouwen betekenen veel voor mij. Gwendolyn, jij zorgde voor (shop)ontspanning in Parijs en verwelkomde mij in je Maastrichtse stulp voor een productieve proefschriftweek. Astrid, jou bedank ik voor de vele gezellige avonden, vaak met een wijntje erbij. Lekker gek doen en je niet gek laten maken lukt altijd goed met jou. Haantjes, ook jullie hebben voor vele mooie momenten gezorgd de afgelopen jaren. Aan onze voormalige maandagavondstek heb ik een kleine ode gebracht in hoofdstuk twee. Eens kijken of ik jullie aan het lezen kan krijgen in een bestuurskundig proefschrift.

Mama, natuurlijk heb ik dit boek aan jou opgedragen. Jij attendeerde mij op de vacature voor promovendus in Tilburg en steunde mij in het sollicitatieproces. Je was blij met mij als ik goede commentaren terugkreeg. Je genoot met me mee als ik naar het buitenland afreisde voor een congres. Je sprak me moed in tijdens moeilijke momenten. Je vond het net als ik niet eerlijk dat je niet bij mijn verdediging zou kunnen zijn. – *Waterfeature* – Tegelijkertijd maakte de gedachte aan die dag je zichtbaar trots. Ik weet zeker dat je zit te glunderen op je wolk, niet in de laatste plaats om wat we ook nu weer als zussen en broer samen doen. Brigitte, Michiel en Mathilde, onze band is onverbreekbaar. Daar heeft mama de fundering voor gelegd. Wij zijn er voor elkaar. Brigitte, ik ben heel trots dat jij de omslagillustratie hebt gemaakt. Het is een krachtig beeld geworden. Michiel, jaren geleden wist ik al dat jij één van mijn paranimfen zou worden. Natuurlijk, omdat ik het leuk vind om mijn broer eens in rokkostuum te zien, en ook omdat het academische podium past bij jouw wetenschappelijke talent. Dan mijn eveneens artistieke zus Mathilde, met trots draag ik tijdens mijn verdediging de creatie van jou en Naomi da Silva. Ook denk ik aan onze vele GG- en G-avonden, die mij de broodnodige ontspanning en afleiding hebben gebracht. Verder bedank ik tante Tilly, evenals Jan, Bob, Joan en Jim voor jullie steun de afgelopen jaren. Familie is voor altijd.

Maar hoe kom ik dan in Parijs terecht? ‘Met de trein, vanuit Bordeaux’, is één van de antwoordopties in het kader van dit proefschrift. Buiten dat kader is er maar één antwoord mogelijk: Robert. Merci pour tout, mon coeur. Je suis ravie de partager mon chemin avec toi.

Parijs, juli 2014

Charlotte van Ooijen

INHOUDSOPGAVE

DEEL I	PUBLIEKE MOBILITEITSSURVEILLANCE IN THEORIE.....	17
HOOFDSTUK 1	PUBLIEKE MOBILITEITSSURVEILLANCE: SAMENSPEL VAN TECHNOLOGIE EN BELEID.....	19
1	Publieke mobiliteitssurveillance in Nederland	19
1.1	Bekende beleidsvraag, nieuwe technologie.....	19
1.2	Veranderingen in de diepte en breedte van overheidsbeleid	21
2	Probleemstelling.....	23
2.1	Publieke mobiliteitssurveillance: gevaar of weldaad?.....	23
2.2	Doelstelling, vraagstelling en centraal concept	24
2.3	Deelvragen	25
3	Wetenschappelijke en maatschappelijke relevantie	28
3.1	Bestuurskundige aanvulling op technisch, juridisch en ethisch onderzoek	28
3.2	Verdieping van e-governmentliteratuur en surveillance studies.....	29
3.3	Maatschappelijke relevantie	32
HOOFDSTUK 2	PUBLIEKE MOBILITEITSSURVEILLANCE IN INFORMATIETECHNOLOGISCHE ZIN.....	35
1	Inleiding.....	35
2	Mobiliteit	35
2.1	Sociale en ruimtelijke mobiliteit	35
2.2	Mobiliteit als tweedimensionaal begrip.....	36
3	Mobiliteitsgegevens: object, plaats en tijd	41
3.1	Inleiding	41
3.2	Objectgegevens: wie/wat...?	42
3.3	Plaatsgegevens: waar...?	43
3.4	Tijdsgegevens: wanneer...?	46
4	Actoren en gegevensstromen in de totstandkoming van mobiliteitsinformatie	47
4.1	De gegevensketen voor mobiliteitsinformatie	47
4.2	Rollen van overheid en burger in de totstandkoming van mobiliteitsinformatie	50
5	Technologieën voor mobiliteitssurveillance.....	51
5.1	Waarnemen en context genereren	51
5.2	Plaatsbepalingstechnologieën.....	52
5.3	Geografische informatiesystemen	59
6	Conclusie	62

HOOFDSTUK 3 DE POLITIEK-BESTUURLIJKE ACHTERGROND VAN PUBLIEKE MOBILITEITSSURVEILLANCE65

1	Inleiding.....	65
2	Kaarten, staten en territoriale grenzen.....	66
2.1	De eerste kaarten: wereldvisie en ontdekkingstochten	66
2.2	Cartografie in de 15 ^e en 16 ^e eeuw: beginnend oog voor politiek en grenzen ..	68
2.3	Cartografie in de 17 ^e en 18 ^e eeuw: groeiende staatscontrole en staatsbelangen.....	70
2.4	Cartografie in de 19 ^e , 20 ^e en 21 ^e eeuw: staten maken kaarten en kaarten maken staten	72
3	Regulering van mobiliteit: de opkomst van het paspoort.....	74
3.1	Introductie van het legitieme recht op beweging.....	74
3.2	Statelijke in- en exclusie: kwestie van gemeenschap en territorium	75
4	Staten onder druk: deterritorialisering	77
4.1	ICT versterkt en accelereert deterritorialisering	77
4.2	Publieke mobiliteitssurveillance en deterritorialisering	79
5	Conclusie	81

HOOFDSTUK 4 SURVEILLANCE IN DE RELATIE OVERHEID-BURGER: CONTROLE, INTERACTIE EN VOORZORG83

1	Inleiding.....	83
2	Legitimiteit als beoordelingscriterium van surveillance	84
2.1	Wat is legitimiteit?	84
2.2	Legaliteit, normatieve rechtvaardiging en maatschappelijke acceptatie	86
3	De relatie overheid-burger.....	87
3.1	Inleiding	87
3.2	De verhouding machthebber-onderdaan.....	88
3.3	De verhouding dienstverlener-cliënt	89
3.4	De verhouding democratisch instituut-citoyen.....	90
3.5	De relatie overheid-burger en surveillanceperspectieven.....	90
4	Het controleperspectief	92
4.1	Big Brother is watching you	92
4.2	Disciplineren in het elektronisch superpanopticon	93
4.3	Assumpties over technologie en legitimiteit	94
4.4	Invulling van de relatie overheid-burger	95
4.5	Mevrouw Smit ervaart surveillance als controle	98
5	Het interactieperspectief	99
5.1	O burgers, deelt en verbindt uw informatie!.....	99
5.2	De logica van social media.....	101
5.3	Assumpties over technologie en legitimiteit	103
5.4	Invulling van de relatie overheid-burger	104
5.5	Mevrouw Smit ervaart surveillance als interactie	106

6	Het voorzorgperspectief	108
6.1	Voorkomen is beter dan genezen	108
6.2	Categorisering van burgers	110
6.3	Assumpties over technologie en legitimiteit	112
6.4	Invulling van de relatie overheid-burger	113
6.5	Mevrouw Smit ervaart surveillance als voorzorg	115
7	Conclusie: theoretische implicaties van surveillance voor de relatie overheid-burger	116
 DEEL II PUBLIEKE MOBILITEITSSURVEILLANCE IN DE PRAKTIJK119		
HOOFDSTUK 5 AANPAK EMPIRISCH ONDERZOEK.....		121
1	Inleiding.....	121
2	Methodologie, onderzoeksbronnen en methoden.....	122
2.1	Methodologie: niet verklaren, maar begrijpen	122
2.2	Onderzoeksbronnen in twee casusonderzoeken	123
2.3	Technieken voor het genereren van onderzoeksgegevens	125
2.4	Positie van de onderzoeker	128
3	Analyse van onderzoeksgegevens	129
HOOFDSTUK 6 AUTOMATISCHE NUMMERPLAATHERKENNING IN DE POLITIETREGIO NODAALSTAD		133
1	Inleiding.....	133
2	Het Nodaalse ANPR-systeem: technologie en organisatie.....	135
3	ANPR: van verkeershandhaving tot opsporing en nodale oriëntatie.....	139
3.1	ANPR voor verkeershandhaving	139
3.2	ANPR voor opsporing	144
3.3	ANPR voor nodale oriëntatie	153
3.4	Recapitulatie.....	172
4	Analyse: surveillanceperspectieven in het ANPR-beleid van de Politie Nodaalstad.....	176
4.1	Technologie- en legitimiteitsassumpties	176
4.2	Koppeling aan surveillanceperspectieven	178
4.3	Implicaties van het Nodaalse ANPR-beleid voor de relatie overheid-burger	187
5	Conclusie	194
HOOFDSTUK 7 INNOVATIE BIJ DE INWINNING EN VERWERKING VAN VERKEERSGEGEVENS		197
1	Inleiding.....	197
2	NDW en de aanloop naar de aanbesteding NON	198

2.1	De Nationale Databank Wegverkeersgegevens	198
2.2	Aanloop naar de aanbesteding NON	202
3	Op zoek naar innovatie	207
3.1	Formuleren van de aanbestedingsvraag.....	207
3.2	Marktconsultatie.....	214
3.3	Publicatie, beoordeling en gunning	215
3.4	Recapitulatie.....	220
4	Analyse: surveillanceperspectieven in het innovatiebeleid van NDW.....	222
4.1	Technologie- en legitimiteitsassumpties	222
4.2	Koppeling aan surveillanceperspectieven	224
4.3	Implicaties van het innovatiebeleid van NDW voor de relatie overheid-burger	233
5	Conclusie	240
HOOFDSTUK 8 CONCLUSIE: HET RISICO VAN DE MOBIELE BURGER..		243
1	Inleiding.....	243
2	ICT en politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance.....	244
2.1	ICT van publieke mobiliteitssurveillance.....	244
2.2	Politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance	247
3	Surveillanceperspectieven in theorie en praktijk.....	248
3.1	Surveillanceperspectieven in theorie	248
3.2	Surveillanceperspectieven in de praktijk van publieke mobiliteitssurveillance.....	252
4	Implicaties van publieke mobiliteitssurveillance voor de manier waarop de overheid haar relatie met de burger vormgeeft	256
5	Discussie en reflectie	260
5.1	Het concept publieke mobiliteitssurveillance en de methodologische benadering hiervan	260
5.2	Waarde van surveillanceperspectieven: descriptie en duiding	261
5.3	Publieke mobiliteitssurveillance en de territorialiteit van de overheid.....	263
LITERATUUR		265
ENGLISH SUMMARY		281
RÉSUMÉ FRANÇAIS		291
INDEX FIGUREN EN TABELLEN		301
BIJLAGE I INTERVIEWGIDS CASUS ANPR-POLITIE		303
BIJLAGE II INTERVIEWGIDS CASUS INNOVATIE-NDW		305
OVER DE AUTEUR.....		307

DEEL I

PUBLIEKE MOBILITEITSSURVEILLANCE IN THEORIE

HOOFDSTUK 1

PUBLIEKE MOBILITEITSSURVEILLANCE: SAMENSPEL VAN TECHNOLOGIE EN BELEID

1 Publieke mobiliteitssurveillance in Nederland

1.1 Bekende beleidsvraag, nieuwe technologie

Wie is waar op welk moment?

Deze vraag naar mobiliteitsinformatie is essentieel voor het functioneren van vele onderdelen van het hedendaagse openbaar bestuur. Ze wordt dan ook vaak gesteld op verschillende niveaus en terreinen van overheidsbeleid in Nederland. Waar houdt verdachte X zich op? Wie zijn onze landsgrenzen overgestoken? Welke geregistreerde voetbalhooligans naderen via de A16? Op welke wegen is het druk met welke categorie voertuigen? Publieke instanties zoals Rijkswaterstaat en de Nederlandse politie zijn voor het uitvoeren van een groot aantal van hun taken afhankelijk van antwoorden op vragen als deze.

Dankzij technologische ontwikkelingen is de vraag naar personen, locaties en tijdstippen tegenwoordig gemakkelijker en gedetailleerder te beantwoorden dan ooit. Onder meer in het veiligheidsbeleid, in de zorg en op het gebied van verkeersmanagement vertrouwt men meer en meer op technologie om te bepalen wie waar wanneer is. Zo stellen camera's met gezichtsherkenning vast welke onruststokers zich op een bepaald moment op de Rotterdamse tramlijn 2 bevinden (NRC Handelsblad, 2010), helpt GPS¹ verzorgers om dementerende ouderen te behoeden voor dwaaltochten (Horjus, Willemse en Pot, 2010) en is in Noord-Brabant verkeersinformatie gegenereerd met behulp van de signalen van mobiele telefoons van weggebruikers (Provincie Noord-Brabant, 2010).

Deze technologische toepassingen zijn te begrijpen als een vorm van surveillance, i.e. 'any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered' (Lyon, 2001a: 2). Voor velen kleeft er een duister element aan het woord surveillance:

¹ GPS is de veel gebruikte afkorting voor het Global Positioning System, een Amerikaans satellietstelsel.

‘The approach of many surveillance scholars involves a form of hermeneutics of suspicion whereby new developments are read negatively as involving inevitable and often cunningly devious expansions and intensifications of surveillance in the service of social control.’

(Haggerty, 2006: 35)

Surveillance hoeft echter niet zonder meer negatief te worden opgevat. In latere publicaties geeft Lyon aan dat surveillance elementen van ‘care’, ‘control’ of een combinatie van beide in zich kan hebben (Lyon, 2007a: 3-4; 2007b: 450). Deze benadering maakt het mogelijk om een bij voorbaat normatieve kwalificatie van surveillance, negatief of positief, terzijde te schuiven. De term surveillance dient hier niet als normatief, maar wel als conceptueel startpunt voor de overheidsactiviteiten die onderwerp zijn van dit proefschrift. Hiermee beoog ik de ernstige beperkingen van een dergelijke normatieve geladenheid ‘in terms of developing an appreciation for the operation of the totality of contemporary surveillance’, waar Haggerty (2006: 35) voor waarschuwt, te vermijden. Het type surveillance dat centraal staat in dit proefschrift duid ik aan met publieke mobiliteitssurveillance,² omdat dit zich afspeelt in het publieke domein en er een specifieke nadruk ligt op de mobiliteitskenmerken van plaats en tijd die persoonsgegevens hebben of krijgen.³ Op het concept publieke mobiliteitssurveillance kom ik in de bespreking van de probleemstelling verderop in dit hoofdstuk uitgebreider terug.

Op zichzelf lijkt het niets nieuws dat de overheid graag wil weten waar burgers gaan en staan. Sinds de opkomst van de moderne West-Europese staten in de 18^e eeuw hebben overheden al activiteiten ontplooid om te controleren wie zich binnen de territoriale grenzen bevinden en wie deze overschrijden. Zo werd het paspoort ingevoerd om vast te kunnen stellen wie een territorium ingaat en wie het verlaat (Torpey, 2000). Deze historisch aanwezige overheidsinteresse in de mobiliteit van burgers is belangrijk om

² Ik heb ervoor gekozen om de in de Angelsaksische literatuur gebruikelijke term surveillance te gebruiken en niet de letterlijke Nederlandse vertaling toezicht. Toezicht heeft in de bestuurskundige literatuur doorgaans een andere betekenis dan surveillance in dit proefschrift. Het begrip toezicht sluit aan bij debatten over verantwoording. In het Engels wordt dit begrip aangeduid als ‘supervision’ of ‘oversight’ en nimmer als ‘surveillance’. Zie onder meer Van Montfort (2010) voor een overzicht van dit onderzoeksgebied.

³ Surveillance die in principe niet gericht is op mobiliteit, kan dit wel worden. Denkt u bijvoorbeeld aan de database van mensen met belastingschulden. Lyons definitie volgens is dit een vorm van surveillance, omdat de opgeslagen persoonsgegevens onder andere worden gebruikt ten behoeve van de managementtaken van de belastingdienst: het heffen van belastingen. Zodra deze database gekoppeld wordt aan een politiedatabase met kentekenregistraties, cameralocaties en tijdstippen van voertuigpassages is er sprake van mobiliteitssurveillance. Op dat moment is namelijk bekend waar de bij de personen behorende auto’s zich op een bepaald moment bevinden. De belastingdienst is dan in staat op die plaats en dat tijdstip de schulden te innen.

de hedendaagse publieke mobiliteitssurveillance te begrijpen. In hoofdstuk 3 ga ik hier verder op in. De opkomst van informatie- en communicatietechnologie (ICT) betekent echter meer dan het ontstaan van nieuwe middelen om bestaande praktijken vorm te geven, zo heeft onderzoek op het gebied van e-government al uitgewezen (Snellen, 2005). Zeker, ICT vult de menselijke zintuiglijke waarneming aan of vervangt deze soms helemaal. Zo wordt de blik van de douanebeambte aangevuld met de lezing van digitale vingerafdrukken op de chip van het biometrisch paspoort en registreren camera's met kentekenherkenning voertuigen bij grensovergangen (Van Elk, 2008). Een al te voluntaristische⁴ visie op ICT verhult echter de fundamentele veranderingen die publieke mobiliteitssurveillance naar verwachting teweegbrengt in overheidsbeleid en daarmee in de relatie tussen overheid en burgers. Zowel in de diepte als in de breedte van overheidsbeleid zijn al enkele veranderingen waar te nemen.

1.2 Veranderingen in de diepte en breedte van overheidsbeleid

Beleidspraktijken zoals verkeersmanagement en grenscontroles, waarbij mobiliteitsinformatie van oudsher al een belangrijke rol speelt, zijn inmiddels tot in de haarvaten doordrongen van ICT. De technologie faciliteert hier de inwinning en verwerking van grotere hoeveelheden mobiliteitsgegevens dan voorheen. Deze toename aan gegevens komt op twee manieren tot stand. Ten eerste maakt ICT het mogelijk om gegevens in te winnen over meer mensen (populatie-uitbreiding). Het oog van de ANPR-camera registreert alle auto's in een file, terwijl de Rijkswaterstaatmedewerker die traditioneel voor dit doel langs de weg staat hier niet toe in staat is. Ten tweede zorgt ICT voor meer waarnemingen per burger per dag (intensivering). De automobilist wordt tijdens zijn rit niet door één, maar door tientallen ANPR-camera's waargenomen en staat daarnaast mogelijk nog mobiliteitsgegevens af via de GPS van zijn navigatiesysteem of het netwerk van zijn telecomprovider. Vervolgens maakt de calculatiefunctie van ICT het mogelijk om ingewikkelde berekeningen uit te voeren op deze grote hoeveelheden gegevens (Bekkers en Zuurmond, 2005: 61). De uitbreiding en intensivering van 'de blik' die resulteert in een toename aan mobiliteitsinformatie heeft naast organisatorische implicaties⁵ mogelijk gevolgen voor het beleid zelf, omdat er een ander beeld ontstaat van de maatschappelijke problemen waar het beleid op is gericht.

⁴ Wetenschappelijke visie die ICT primair beschouwt als middel dat een actor ter hand kan nemen om een bepaald doel te bereiken. De voluntaristische visie is de tegenhanger van de deterministische visie die ervan uitgaat dat technologische ontwikkelingen het handelen van actoren aansturen. Zie voor een uitgebreidere beschrijving van het technologiedebat onder meer (Bekkers, Lips en Zuurmond, 2005b: 38-40) en (Frissen, 1996: 55-57).

⁵ Zie onder meer Zuurmond (1994) en Bovens & Zouridis (2002) voor een bestuurskundige analyse van de implicaties van ICT voor overheidsorganisaties.

Vervolgens vraagt dit van de betrokken beleidsactoren om een heroriëntatie op het beleid (in uitvoering). Haggerty (2006: 41) zegt hierover:

‘Indeed, surveillance in various forms is recognized as being among the most important technologies of governance, as new ways of “seeing” a population can open up new ways of conceptualizing the aims of governance and its practical possibilities.’

De vaststelling dat bestaande beleidsvragen op een nieuwe manier worden beantwoord doet het karakter van publieke mobiliteitssurveillance daarom te kort. De opkomst van surveillancetechnologie zorgt ervoor dat bestaande beleidsvragen nieuwe, technologisch gegenereerde antwoorden krijgen en tegelijkertijd dat technologisch gegenereerde antwoorden nieuwe beleidsvragen oproepen. Zo zou de slimme energiemeter mogelijk het technologische antwoord op de vraag naar energiebesparing zijn, maar tegelijkertijd de interesse wekken van politie en inlichtingen- en opsporingsdiensten (Cuijpers, 2011).

Met de toename aan technische mogelijkheden om persoons-, locatie- en tijdsgegevens in te winnen en te verwerken, lijkt ook de vraag naar deze gegevens vaker en vanuit meer beleidsterreinen gesteld te worden dan voorheen. Illustratief voor deze verandering in de breedte van overheidsbeleid is het wetsvoorstel kilometerprijs dat op 13 november 2009 door het kabinet Balkenende IV wordt goedgekeurd.⁶ Dit wetsvoorstel van toenmalig minister van Verkeer en Waterstaat Camiel Eurlings stelt een alternatief systeem voor de motorrijtuigenbelasting voor. In plaats van een systeem van belastingheffing dat gebaseerd is op het bezit van een voertuig, gaat het nieuwe systeem uit van het verbruik van een voertuig (Ministerie van Verkeer en Waterstaat, 2009). Het wetsvoorstel geeft aan dat de te betalen gebruiksafhankelijke prijs wordt berekend aan de hand van drie hoofdtypen van gegevens (Tweede Kamer der Staten-Generaal, 2009). Allereerst gaat het om milieuvriendelijkheidscriteria, zoals de koolstofdioxide-uitstoot en de ledige massa, waarmee het toepasselijke basistarief berekend kan worden. Een tweede type gegevens betreft het aantal gereden kilometers. Ten derde moet bekend zijn op welke categorie wegen de kilometers zijn verreden om te kunnen bepalen over hoeveel kilometers naast het basistarief het spitstarief verschuldigd is. Voor het tweede en derde criterium wil het ministerie gebruik maken van een kastje dat gegevens over de gemaakte voertuigbewegingen opslaat. Om een voertuig te kunnen belasten moeten derhalve data worden ingewonnen over de locaties en tijdstippen waarop dit zich begeeft. De vraag ‘waar is auto x’ wordt op enig moment

⁶ Met de val van het kabinet-Balkenende IV in februari 2010 is het wetsvoorstel kilometerprijs controversieel verklaard. Dit betekent dat de behandeling van het wetsvoorstel in het parlement moest wachten tot na de verkiezingen van juni 2010.

gesteld in het calculeren van de kilometerprijs. Dit voorbeeld laat zien dat voor beleid dat tot dusver geen mobiliteitscomponent in zich had nu wordt ingezet op plaatsbepalingstechnologie om beleidsdoelstellingen te realiseren.⁷

2 Probleemstelling

2.1 Publieke mobiliteitssurveillance: gevaar of weldaad?

De implicaties van publieke mobiliteitssurveillance in de diepte en breedte van overheidsbeleid roepen vragen op over de positie van burgers ten opzichte van de overheid. Technologiepessimisten zien een groot gevaar voor burgers. De overheid zou wel eens te veel macht kunnen krijgen door mobiliteitssurveillance. Macht gaat immers van oudsher al om het beheersen van ruimte, tijd en beweging.⁸ De mogelijkheden hiertoe zijn met publieke mobiliteitssurveillance exponentieel toegenomen. Extreme vormen van controle en beperkingen van de bewegingsvrijheid van burgers zouden dreigen (Dobson en Fisher, 2003). Taylor, Lips en Organ (2009) merken echter op dat een dergelijke pessimistische visie geen ruimte laat voor het profijt dat burgers kunnen hebben van technologische ontwikkelingen in termen van betere overheidsdienstverlening. Maar wat schieten we op met de vaststelling dat een technologische toepassing zoals de kilometerprijs zowel een gevaar als een weldaad zou kunnen zijn voor burgers? Wat leren technologische mogelijkheden ons over wat publieke mobiliteitssurveillance in de praktijk betekent voor de positie van burgers ten opzichte van de overheid? In hoeverre de soms gedroomde en soms gevreesde potentie van de technologie daadwerkelijk tot uiting komt in overheidsbeleid is vaak vrij onzeker. Pas als er meer inzicht bestaat in het proces waarlangs mobiliteitssurveillance in overheidsbeleid tot stand komt en hoe ze zich vervolgens manifesteert, zijn er zinnige uitspraken te doen over wat publieke mobiliteitssurveillance betekent voor de relatie tussen overheid en burger.⁹

⁷ Evenwel zal dit beleid – in ieder geval voorlopig – niet ten uitvoer worden gebracht, omdat het expliciet is afgewezen in het regeerakkoord van het kabinet-Rutte II (Rijksoverheid, 2012b). Dit gegeven doet echter geen afbreuk aan de illustratieve waarde van dit voorbeeld voor de relatie tussen beleid en technologie.

⁸ Hier ga ik in hoofdstuk 3 verder op in.

⁹ Mobiliteitssurveillance speelt niet alleen in relaties tussen overheid en burger, maar ook tussen overheid en overheid, burger en burger, en bedrijven en burgers. De focus van dit proefschrift ligt op publieke mobiliteitssurveillance in de relatie overheid-burger. Waar relevant worden toepassingen in de andere typen relaties wel genoemd, maar deze zijn nimmer object van analyse.

2.2 Doelstelling, vraagstelling en centraal concept

Het doel van dit proefschrift is tweeledig. Allereerst richt ik mij met het onderhavige onderzoek op het verkrijgen van inzicht in de manier waarop publieke mobiliteitssurveillance betekenis krijgt in overheidsbeleid. Hiermee moet duidelijk worden op welke manier technologische mogelijkheden en onmogelijkheden doorwerken in de beleidspraktijk. Ten tweede beoog ik met dit onderzoek een conceptueel raamwerk te ontwikkelen om de implicaties van publieke mobiliteits-surveillance voor de relatie overheid-burger te duiden vanuit een beleidsperspectief. Dit raamwerk dient om zowel kansen als eventuele spanningen bloot te leggen die als gevolg van de toepassing van de betrokken technologieën ontstaan in de relatie overheid-burger. De onderzoeksresultaten kunnen vervolgens als aandachtspunten fungeren bij de verdere ontwikkeling van mobiliteitssurveillance in het openbaar bestuur evenals het maatschappelijk en wetenschappelijk debat hierover. Om deze twee onderzoeksdoelstellingen te realiseren, heb ik de volgende centrale onderzoeksvraag geformuleerd:

Wat zijn de implicaties van publieke mobiliteitssurveillance voor de manier waarop de overheid haar relatie met de burger vormgeeft?

Wat publieke mobiliteitssurveillance betekent voor de relatie tussen overheid en burgers bezie ik in dit proefschrift vanuit het perspectief van de overheid. De manier waarop de burger invulling geeft aan zijn relatie met de overheid in het licht van publieke mobiliteitssurveillance valt derhalve buiten de reikwijdte van dit onderzoek.

Publieke mobiliteitssurveillance is geen nieuw fenomeen in de praktijk van het openbaar bestuur, maar wel een nieuw concept in de studie van het openbaar bestuur. Wat ik in dit proefschrift aanduid als publieke mobiliteitssurveillance staat derhalve noch binnen het openbaar bestuur zelf, noch in de bestuurskunde als zodanig bekend. Uiteenlopende beleidspraktijken, zoals cameratoezicht in de stad, GPS-lokalisatie van tbs-veroordeelden¹⁰ of GSM-tracking van 112-bellers, worden te beperkt besproken in de samenhang die ik ze wil toedichten. Verderop in dit proefschrift zal duidelijk worden dat deze samenhang vanuit zowel informatietechnologisch als politiek-

¹⁰ De afkorting tbs staat voor terbeschikkingstelling. Tbs is 'een behandelaatregel die de rechter oplegt aan mensen die zware delicten hebben gepleegd en lijden aan een psychiatrische ziekte of stoornis' (Openbaar ministerie, 2014).

bestuurlijk oogpunt te motiveren is.¹¹ Een lastig aspect van het werken met een nieuw concept, is dat er nog geen definitie van bestaat. Om toch voldoende inkadering en richting te geven aan dit onderzoek, maak ik gebruik van een werkdefinitie. Op basis van de eerder genoemde definitie van surveillance van David Lyon definieer ik publieke mobiliteitssurveillance voorlopig als volgt:

Het op digitale wijze verzamelen en verwerken van mobiliteitsgegevens over al dan niet identificeerbare personen, teneinde personen en populaties voor publieke doeleinden te beïnvloeden of te sturen.

Deze werkdefinitie dient als uitgangspunt om het fenomeen publieke mobiliteitssurveillance in de volgende hoofdstukken theoretisch en empirisch te kunnen verkennen.

De centrale onderzoeksvraag werk ik uit in vijf deelvragen. Om de deelvragen en uiteindelijk de hoofdvraag te beantwoorden, voer ik een literatuurstudie uit en verricht ik empirisch onderzoek.

2.3 Deelvragen

2.3.1 Deel I Publieke mobiliteitssurveillance in theorie

In het eerste deel van dit proefschrift volgt het verslag van het literatuuronderzoek naar publieke mobiliteitssurveillance, waarmee de werkdefinitie theoretisch wordt uitgewerkt. Het literatuuronderzoek heb ik vormgegeven aan de hand van de drie volgende deelvragen.

Deelvraag 1 - Wat is publieke mobiliteitssurveillance in informatietechnologische zin?

Deze vraag staat centraal in hoofdstuk 2. Met het beantwoorden van deze vraag wordt het eerste deel van de werkdefinitie van publieke mobiliteitssurveillance uitgediept: *het op digitale wijze verzamelen en verwerken van mobiliteitsgegevens over al dan niet identificeerbare personen*. Ik leg uit wat mobiliteitsgegevens over al dan niet identificeerbare personen zijn en op welke manieren deze gegevens digitaal verzameld en verwerkt kunnen worden. De bespreking baseer ik hoofdzakelijk op literatuur over

¹¹ Dit punt werk ik achtereenvolgens uit in de hoofdstukken 2 en 3.

location-based services (LBS). Daarnaast put ik uit inzichten uit de geoinformatiewetenschappen en informatica. Ik werk het begrip mobiliteit uit en besteed aandacht aan de datastromen, technologie-actoren en technologieën die publieke mobiliteitssurveillance in technische zin mogelijk maken.

Deelvraag 2 - Wat is de politiek-bestuurlijke achtergrond van publieke mobiliteits-surveillance?

Hoofdstuk 3 is geheel gewijd aan het beantwoorden van deze vraag. Evenals de vorige deelvraag dient deze vraag om meer theoretisch inzicht te verwerven in het fenomeen publieke mobiliteitssurveillance. Hierbij geef ik vanuit historisch perspectief invulling aan de werkdefinitie. Zo wordt inzichtelijk vanuit welke politiek-bestuurlijke achtergrond de overheid belangstelling heeft gekregen voor mobiele burgers. De wil tot weten en het in kaart brengen van locaties en bewegingen van burgers door de overheid belicht ik vanuit literatuur over de historisch gegroeide politieke betekenis van kaarten, de opkomst van het paspoort en de relatie tussen ICT en territorialiteit.

Deelvraag 3 - Welke perspectieven op surveillance in de relatie overheid-burger kunnen worden onderscheiden?

Nadat in de hoofdstukken 2 en 3 duidelijk is geworden wat publieke mobiliteits-surveillance vanuit informatietechnologisch en politiek-bestuurlijk oogpunt inhoudt, is het tijd om in hoofdstuk 4 het tweede deel van de hoofdvraag, *implicaties voor de manier waarop de overheid haar relatie met burgers vormgeeft*, theoretisch te onderzoeken. Hoe kunnen deze implicaties eruit zien? Om dit inzichtelijk te maken, koppel ik theorievorming over legitimiteit aan drie perspectieven op surveillance (controle, interactie en voorzorg). Vervolgens beredeneer ik vanuit ieder surveillanceperspectief hoe drie verhoudingen tussen overheid en burger (machthebber-onderdaan, dienstverlener-cliënt en democratisch instituut-citoyen) theoretisch kunnen worden ingevuld. Het resultaat van het hoofdstuk is een theoretisch raamwerk met mogelijke implicaties van surveillance voor de relatie overheid-burger. Hiermee wordt invulling gegeven aan het tweede deel van de werkdefinitie van publieke mobiliteitssurveillance: *teneinde personen en populaties voor publieke doeleinden te beïnvloeden of te sturen*.

2.3.2 Deel II Publieke mobiliteitssurveillance in de praktijk

Na de literatuurstudie volgt in deel II van dit proefschrift het verslag van het empirisch onderzoek. Dit begint in hoofdstuk 5 met een toelichting op en verantwoording van de onderzoeksmethodologie. Ik ga hier onder andere in op de selectie van twee casussen van publieke mobiliteitssurveillance. Ook presenteer ik de gebruikte onderzoekstechnieken om het empirische materiaal te ontsluiten en leg ik uit hoe ik tot een analyse van het materiaal kom.

De deelvragen 4 en 5 geven richting aan het empirisch onderzoek.

Deelvraag 4 - In hoeverre komen de verschillende surveillanceperspectieven voor in de beleidspraktijk van publieke mobiliteitssurveillance?

Deelvraag 5 - Welke invulling van de relatie overheid-burger vloeit voort uit de in de beleidspraktijk aangetroffen kenmerken van de surveillanceperspectieven?

De empirische verkenning van publieke mobiliteitssurveillance vindt plaats in de vorm van twee casusonderzoeken in de Nederlandse publieke sector. De eerste casestudy betreft de inzet van automatische nummerplatherkenning (ANPR) door een Nederlands politiekorps (hoofdstuk 6). In de tweede casestudy verruil ik het veiligheidsdomein voor de context van het verkeersmanagement. Innovatieve technieken voor de inwinning en verwerking van verkeersgegevens in Noord- en Oost-Nederland staan daarbij centraal (hoofdstuk 7). Beide hoofdstukken beginnen met een beschrijving van het beleidstraject rondom de publieke mobiliteitssurveillance in de betreffende beleidspraktijken. Vervolgens presenteer ik de resultaten van de interpretatieve beleidsanalyse die ik voor beide casussen heb uitgevoerd. Deze resultaten moeten duidelijk maken in hoeverre de in hoofdstuk 4 uitgewerkte surveillanceperspectieven voorkomen in de onderzochte beleidspraktijken en wat dit betekent voor de invulling van de relatie tussen overheid en burger.

In hoofdstuk 8 breng ik de opgedane theoretische en empirische inzichten samen en formuleer ik een antwoord op de centrale onderzoeksvraag. Tenslotte geef ik een reflectie op het verrichte onderzoek.

Waarom is het van belang om een antwoord op de centrale onderzoeksvraag te vinden? Kortom, welke bijdrage beoog ik met dit proefschrift te leveren aan welke wetenschappelijke en maatschappelijke debatten?

3 Wetenschappelijke en maatschappelijke relevantie

3.1 Bestuurskundige aanvulling op technisch, juridisch en ethisch onderzoek

Het wetenschappelijk debat rondom de opkomst van wat ik publieke mobiliteits-surveillance noem, lijkt zich met name te concentreren op de technische (Raper, Gartner, Karimi et al., 2007), juridische (Nouwt, 2008; Nouwt en Van der Wees, 2008; Smits, 2008) en ethische (Michael, Fusco en Michael, 2008; Onsrud, 2008) mogelijkheden en onmogelijkheden van technologie. Dankzij bijdragen uit disciplines zoals geo-informatiewetenschap en informatica weten we steeds beter wat er qua techniek wel en niet gerealiseerd kan worden.¹² Zo is bekend dat een mobiele telefoon in stedelijk gebied op 50 tot 500 meter nauwkeurig te positioneren is als je de meetmethode op basis van Cell-ID gebruikt (Brimicombe en Li, 2009: 190). Ook weten we dat de locatiegegevens van mobiele telefoons in een Geografisch Informatiesysteem (GIS) gevisualiseerd kunnen worden om bijvoorbeeld de bewegingen van toeristen in Rome te bekijken (Calabrese en Ratti, 2006). De mobiliteitsgegevens van verschillende gebruikers kunnen vervolgens in een geografisch informatiesysteem weergegeven worden, zodat er een plaatje ontstaat van het gedrag van de te analyseren personen (Ahas en Mark, 2005). Dit scala aan technologisch georiënteerd onderzoek zegt echter niets over de mate waarin deze ontwikkelingen juridisch en ethisch toelaatbaar zijn. Aan vragen over de juridische en ethische grenzen wordt ruimschoots aandacht besteed in de law & technology-literatuur (zie onder meer Koops, Leenes en De Hert, 2008). Een veelgestelde vraag is hier in hoeverre het gebruik van surveillancetechnologie een al dan niet gelegitimeerde inbreuk maakt op grondrechten zoals het recht op privacy.

Dankzij genoemd onderzoek is steeds meer bekend over wat technologisch kan en niet kan en wat vanuit juridisch en ethisch perspectief mag en niet mag. Hiermee is het echter nog niet duidelijk in hoeverre deze mogelijkheden en begrenzingen doorwerken in de beleidspraktijk en ook niet hoe beleidsmakers handelen in situaties waarin de legitimiteitseisen niet helder of zelfs tegenstrijdig zijn. Hoe gaan beleidsmakers om met het aanbod aan verschillende technologieën met de bijbehorende mogelijkheden en beperkingen? Hoe zwaar wegen juridische, ethische en maatschappelijke legitimiteits-aspecten voor beleidsmakers die beïnvloeden hoe de technologie gebruikt wordt? Zijn privacyoverwegingen bijvoorbeeld doorslaggevend om de toepassing van een bepaalde technologie te beperken of wegen andere belangen zoals organisatorische of politieke

¹² Er is sinds 2007 zelfs een Journal of Location Based Services dat vanuit diverse disciplines bijdragen verwelkomt over locatiegebonden technologie. Tot nu toe zijn de bijdragen overwegend technologisch van aard en zijn er weinig artikelen uit de sociale of juridische wetenschappen.

wellicht zwaarder? In een themanummer van het tijdschrift *Surveillance & Society* over surveillance en mobiliteit geven de artikelen van Gow en Inaht (2004) en Green en Smith (2004) inzicht in dergelijke beleidsimplicaties van publieke mobiliteits-surveillance. Gow en Inaht (2004) laten zien hoe zorgen over privacyrechten werden meegenomen in de Canadese beleidsontwikkeling over noodhulpdiensten voor mobiele telefoongebruikers. Green en Smith (2004) baseren hun observaties over de Britse regelgeving rondom mobiele communicatie op interviews met belanghebbenden. De genoemde onderzoekerduo's geven met hun analyses van beleidspraktijken een waardevolle bijdrage aan de kennis over publieke mobiliteitssurveillance, één die navolging verdient.

In mijn optiek is de gevoerde maatschappelijke en wetenschappelijke discussie vaak te zeer geënt op de technologische, juridische en ethische mogelijkheden en bezwaren en is deze te weinig empirisch gefundeerd. Zodoende krijgt de discussie al snel een normatief karakter, waarbij surveillance bijvoorbeeld slecht zou zijn, omdat de privacy van burgers mogelijk wordt geschaad of juist goed omdat burgers hierdoor zouden kunnen genieten van gepersonaliseerde services. Privacy kan echter ook worden gezien als 'sleutelgatbegrip', zoals Wim van de Donk zo mooi uiteenzette in zijn lezing op het Landelijk Congres der Bestuurskunde 2010 (LCB, 2010). Hiermee doelde hij op de achterliggende problematiek van het begrip privacy voor bestuurskundigen. Volgens Van de Donk gaat het om fundamentele vragen over de verhoudingen tussen overheid en burgers en burgers onderling in onze rechtstaat. Hij sprak de verwachting uit dat de massale digitalisering, opslag, uitwisseling en toepassing van persoonsgegevens in beleid de onderlinge verhoudingen flink zal veranderen en daarmee de fundamentele van onze rechtsstaat raakt. Bestuurskundig onderzoek kijkt door het sleutelgat naar de beleidspraktijk en maakt het zodoende mogelijk om meer genuanceerde en empirisch gefundeerde uitspraken over de aard en implicaties van surveillance te doen. Vanuit de overtuiging dat bestuurskundig onderzoek nodig is om de implicaties van publieke mobiliteitssurveillance voor de relatie overheid-burger te duiden richt dit onderzoek zich op het verwerven van inzicht in de beleidsvorming die hiermee verweven is. Hiermee bevind ik mij op het terrein van zowel e-governmentonderzoek als *surveillance studies*.

3.2 Verdieping van e-governmentliteratuur en surveillance studies

In de literatuur over de betekenis van ICT voor het openbaar bestuur, ook wel e-governmentliteratuur genoemd, zijn op hoofdlijnen drie aandachtsgebieden te onderscheiden: beleidsuitvoering, publieke dienstverlening en interactieve beleidsvorming (Snellen, 2005). Deze aandachtsgebieden belichten ieder een andere

dimensie van de relatie overheid-burger. In het denken over beleidsuitvoering staat de burger als onderdaan centraal, bij publieke dienstverlening is deze cliënt en bij interactieve beleidsvorming heeft de burger de rol van citizen.¹³ In het denken over de invloed van ICT op de relatie overheid-burger is een polarisering in het debat waar te nemen. Hierbij zijn drie polen te onderscheiden: Orwell, Athene en Soft Sister.

De eerste twee polen worden weergegeven in de titel van de bundel *Orwell of Athene* (Frissen, Koers en Snellen, 1992). In hun bijdrage aan deze bundel bieden Van de Donk en Tops (1992) een uitgebreid overzicht van de literatuur die vanaf het eind van de jaren zeventig verschijnt over de relatie tussen informatisering en democratie. De auteurs beschrijven de scenario's van een machtige Orwelliaanse staat aan de ene kant en een democratische, Atheense geïnspireerde samenleving aan de andere kant, die zouden worden gefaciliteerd door de ICT-revolutie. Ieder scenario benadrukt andere rollen die overheid en burger ten opzichte van elkaar vervullen. In het Orwell-scenario is de overheid te zien in de rol van Big Brother die de burger dankzij ICT hoofdzakelijk in de rol van onderdaan dwingt. De overheid zou over de macht beschikken om het gedrag van burgers in te perken en te verzekeren dat zij gehoorzamen aan de wil van de staat. De toenemende transparantie van burgers, die veroorzaakt wordt door ICT, zou de sturing en controle van de samenleving faciliteren. Technologie stelt de overheid in staat om afwijkend gedrag gemakkelijk te detecteren en hierop te reageren. ICT wordt zo een wapen waarmee de overheid macht kan uitoefenen over burgers. In de Atheense staat manifesteert de burger zich vooral als citizen. Waar de Orwellianen verwachten dat de staat de ICT-revolutie aangrijpt ter versterking van diens macht en controle over het gedrag van burgers, schetst het Athene-scenario juist een samenleving waarin burgers dankzij de informatisering hun stem beter kunnen laten horen en gelden. In Athene manifesteren burgers zich als citizens in hun relatie met de overheid. In deze rol zijn burgers actief als initiators van beleid en worden ze tegelijkertijd behandeld als partners in het beleidsvormingsproces. Hun meningen doen ertoe en kunnen nu gemakkelijker dan ooit worden gepeild dankzij ICT. Het ideaal van directe democratie ligt dan ook binnen handbereik. Als citizens hebben burgers het recht om zich te bemoeien met en betrokken te worden bij de publieke zaak. ICT faciliteert nieuwe manieren voor de overheid om burgers bij haar activiteiten te betrekken. Vanuit deze optiek wordt ICT vooral gebruikt ten behoeve van samenwerking met burgers.

Een later verschenen overzichtswerk onder redactie van Lips, Bekkers en Zuurmond (2005) sluit af met een vergelijkbare tweedeling als Orwell en Athene onder de aansprekende noemer 'januskop van ICT'. Deze januskop, bestaande uit verticalisering

¹³ De drie burgerrollen van onderdaan, cliënt en citizen werk ik in hoofdstuk 4 verder uit.

in de vorm van intelligente beheersing en infocratie tegenover horizontalisering in de vorm van participatie en zelfrealisatie (Bekkers, Lips en Zuurmond, 2005a: 745) representeert echter voor een deel dezelfde benadering van burgers als Orwell en Athene. Het verticaliseringsscenario verschilt namelijk van het Orwell-scenario door de repressieve rol van de overheid in één adem te noemen met de dienstverlenende rol van de overheid en hier vervolgens de deels corresponderende burgerrollen van klant en kiezer bij te noemen. De rol van klant – cliënt in dit onderzoek – onderscheidt een aantal auteurs echter als derde pool in het debat. Deze wordt treffend verwoord door Taylor, Lips en Organ (2009). Deze auteurs maken een onderscheid tussen onderzoek naar de ‘surveillance state’ en de ‘service state’. Het eerste type onderzoek is overwegend geïnspireerd door de angst voor de reeds genoemde Orwelliaanse staat. De ‘service state’, door Frissen (1998) elegant aangeduid als ‘Soft Sister’ benadrukt de dienstverleningsrelatie tussen overheid en burger. De overheid zou dankzij ICT als een Soft Sister betere diensten kunnen leveren aan de burger als cliënt. Als cliënt verwacht en eist de burger een bepaald dienstverleningsniveau van de overheid. ICT biedt nieuwe manieren om te voorzien in deze behoefte door de kwantiteit en de kwaliteit van publieke diensten te verbeteren. Daarnaast is het streven om diensten zoveel mogelijk op maat aan te bieden aan de individuele cliënt. De overheid zet ICT dan ook in om ten gunste van burgers te handelen.

Zowel Van de Donk en Tops (1992) als Taylor, Lips en Organ (2009) benadrukken terecht de wenselijkheid van het depolariseren van het wetenschappelijk debat over ICT en openbaar bestuur. Orwell versus Athene en de surveillancestaat versus de servicestaat geven een niet tevredenstellend inzicht in de empirische ontwikkelingen rondom surveillance in het openbaar bestuur. Een beperking van de beschreven e-governmentscenario’s is dat ze ieder eenzijdig gefocust zijn op een bepaalde burgerrol. Orwell benadert de burger als onderdaan, in Athene is de burger citoyen en Soft Sister richt zich op de burger als cliënt. Om de implicaties van publieke mobiliteitssurveillance voor de relatie overheid-burger te *begrijpen* is het echter nodig om alle drie de burgerrollen en bijbehorende overheidsrollen nader te bekijken. Door de verhoudingen tussen overheid en respectievelijk onderdaan, cliënt en citoyen niet als normatieve uitersten te beschouwen, maar te erkennen dat deze in ieder surveillancebeleidstraject verschillend ingevuld kunnen worden, beoog ik nuance aan te brengen in het gepolariseerde debat.¹⁴

In het begin van dit hoofdstuk heb ik er al op gewezen dat het onderzoeksveld van *surveillance studies* eveneens gebukt gaat onder een normatieve geladenheid. Deze valt

¹⁴ In hoofdstuk 4 werk ik de mogelijke invulling van de verhoudingen tussen overheid en burger theoretisch uit.

enerzijds toe te schrijven aan een overdaad aan op Jeremy Bentham's panopticon geïnspireerde theorieën: 'The panopticon refuses to go away. Despite the appearance of a number of critiques, the idea of the panopticon still appears routinely in surveillance discourses' (Lyon, 2006b: 4). Binnen de *surveillance studies* gaan expliciet stemmen op om de bestudering van surveillance niet louter vanuit het panopticonperspectief vorm te geven (Haggerty, 2006; Zurawski, 2007). Anderzijds is er een gebrek aan empirisch onderzoek naar de praktijk van surveillance en de actoren die hierbij een rol spelen. Dubbeld (2006) laat in haar analyse van surveillancepraktijken in de gezondheidszorg overtuigend zien dat surveillance studies in theoretisch en methodologisch opzicht veel te winnen hebben bij een actorgerichte benadering. Met dit proefschrift beoog ik bij te dragen aan de theoretische verbreding en empirische versterking van *surveillance studies*.

3.3 Maatschappelijke relevantie

Met dit onderzoek wil ik niet alleen een bijdrage leveren aan de wetenschappelijke kennis over surveillance en e-government, maar ook iets betekenen voor de praktijk van publieke mobiliteitssurveillance. Op welke manieren is dit onderzoek nu maatschappelijk relevant?

Ten eerste helpt de introductie en uiteenzetting van het begrip publieke mobiliteitssurveillance beleidsmakers op nationaal en lokaal niveau om de samenhang tussen verschillende overheidsactiviteiten en de versnipperde inzet van surveillance-technologieën beter te zien. Vervolgens kunnen ze bepaalde overkoepelende problemen, bijvoorbeeld op het gebied van legitimiteit, beter aan te pakken. Het biedt zodoende een kader dat beleids- noch technologiespecifiek is en daarmee een gemeenschappelijke taal voor alle publieke functionarissen die betrokken zijn bij publieke mobiliteitssurveillance.

Het gemeenschappelijke kader dat het concept publieke mobiliteitssurveillance biedt, is ook van belang voor een andere belangrijke groep van betrokken actoren: burgers. Voor burgers is het waardevol om te weten dat overheidsinzet van zaken als cameratoezicht, de ov-chipkaart en mobiele telefoonlokalisatie weliswaar niet in een overkoepelend gecoördineerd systeem gebeurt, maar dat deze toepassingen wel gemeenschappelijke kenmerken hebben met gemeenschappelijke betekenissen voor burgers. Een dergelijk inzicht biedt burgers de mogelijkheid het publieke debat anders aan te gaan dan bij een geïsoleerde benadering van dergelijke toepassingen.

Naast de introductie van het concept heeft de bestuurskundige benadering daarvan meerwaarde voor de maatschappelijke en beleidsmatige discussie. Dit onderzoek draagt bij aan het verkrijgen van inzicht in de rol van de actoren en organisaties die betrokken zijn bij publieke mobiliteitssurveillance. Hierdoor wordt het mogelijk een debat te voeren dat verder gaat dan het bespreken van mogelijkheden en onmogelijkheden, angsten en dromen, hoop en vrees.

HOOFDSTUK 2

PUBLIEKE MOBILITEITSSURVEILLANCE IN INFORMATIETECHNOLOGISCHE ZIN

1 Inleiding

Dit hoofdstuk geeft een antwoord op de vraag: wat is publieke mobiliteitssurveillance in informatietechnologische zin? In hoofdstuk 1 heb ik publieke mobiliteitssurveillance voorlopig gedefinieerd als *‘het op digitale wijze verzamelen en verwerken van mobiliteitsgegevens over al dan niet identificeerbare personen, teneinde personen en populaties voor publieke controle- of dienstverleningsdoeleinden te beïnvloeden of te sturen’*. Vanuit informatietechnologisch perspectief ligt de nadruk op het uitwerken van het eerste, cursief gedrukte deel van de definitie. Het is dan ook van belang om te weten wat mobiliteitsgegevens zijn en hoe het op digitale wijze verzamelen en verwerken hiervan in zijn werk kan gaan. Mobiliteitsgegevens zijn logischerwijs gegevens over mobiliteit. Om te begrijpen wat mobiliteitsgegevens zijn, moet dan ook eerst duidelijk zijn wat mobiliteit is. Vervolgens bespreek ik drie categorieën mobiliteitsgegevens: object, plaats en tijd. In de volgende paragraaf is aandacht voor de actoren en datastromen die een rol spelen in de totstandkoming van mobiliteitsinformatie. Daarna behandel ik een scala aan technologieën waarmee mobiliteitsinformatie geproduceerd kan worden tezamen met enkele toepassingen in het openbaar bestuur. Dit hoofdstuk besluit met een conclusie waarin ik de besproken onderwerpen samenbreng in een antwoord op de gestelde deelvraag.

2 Mobiliteit

2.1 Sociale en ruimtelijke mobiliteit

Mobiliteit kan zowel een sociologische als een ruimtelijke betekenis hebben. Beide betekenissen zijn, soms los van elkaar en soms verweven, terug te vinden in literatuur over mobiliteit en technologie. Soenens (2006: 34) geeft aan dat sociale mobiliteit betrekking heeft op veranderingen in iemands sociaaleconomische status, zoals een beweging van de ene sociale groep naar de andere. Zowel individuele inspanningen als demografische ontwikkelingen kunnen dergelijke verschuivingen veroorzaken, aldus

Soenens (2006: 34). Daarnaast kunnen technologische ontwikkelingen van invloed zijn op sociale mobiliteit:¹⁵

‘With e-mail and texting, we are more able to maintain large, spatially separated networks that can be key to social and other mobilities [...] traditional class structures and the barriers they imposed have been dismantled. Access to information has also meant that traditional gender-based structures that result, for example, in inequalities of jobs and pay and the notorious “glass ceiling” in the promotion of women employees are also being chipped away.’

(Brimicombe en Li, 2009: 16)

Besprekingen over de relatie tussen technologie en mobiliteit gaan echter vaker over ruimtelijke dan sociale mobiliteit. Zo merkt Geser (2004) op dat ‘wireless transmission technologies are certainly at the root of all innovations that make communication compatible with spatial mobility’. Doorgaans wordt in de wetenschappelijke literatuur, net als in het dagelijks spraakgebruik, het bijvoeglijk naamwoord ‘ruimtelijk’ achterwege gelaten. Auteurs hebben het simpelweg over mobiliteit waar ze ruimtelijke mobiliteit bedoelen (zie onder meer Bennett en Regan, 2004; Soenens, 2006). Als het gaat om sociale mobiliteit wordt het meestal ook als zodanig aangeduid. In dit proefschrift volg ik deze manier van aanduiden. Wat is dan (ruimtelijke) mobiliteit? Bennett en Regan (2004: 451) geven in hun bespreking van surveillance en mobiliteit aan dat mobiliteit in de kern om ‘movement’ draait. Hieraan koppelen zij een tweedimensionale typologie van mobiliteit, bestaande uit het surveillanceobject en de beweging zelf.

2.2 Mobiliteit als tweedimensionaal begrip

2.2.1 *Dimensie 1: het surveillanceobject; wat beweegt er?*

De eerste dimensie gaat over de vraag ‘wat beweegt er?’. Binnen deze dimensie stellen Bennett en Regan (2004: 451) drie categorieën voor: lichaam (de persoon), actie¹⁶ (dingen die de persoon doet, hetzij als fysieke handeling, hetzij zoals vastgelegd in

¹⁵ Hoewel sociale mobiliteit en sociale classificatie geen synoniemen zijn van elkaar, sluiten de ideeën van Lyon (2007b) over social sorting als implicatie van surveillance goed aan bij de gedachtevorming over sociale mobiliteit en technologie. In hoofdstuk 4, paragraaf 6.2 ga ik hier verder op in.

¹⁶ Hoewel de auteurs deze categorie aanduiden als ‘transaction’, is de brede betekenis van het Nederlandse ‘actie’ hier meer van toepassing dan ‘transactie’.

data), en artefact (voorwerp dat met het individu wordt geassocieerd). Volgens de auteurs duidt deze eerste dimensie het object of de objecten van surveillance aan. Dit is een zinvolle categorisering, die echter nog wel wat vragen oproept. Wat in een bepaalde situatie nu precies het object van surveillance is, is regelmatig dubbelzinnig. Wanneer bijvoorbeeld de politie in een moordonderzoek locatiegegevens van mobiele telefoons opvraagt, wat is dan het surveillanceobject? Zijn dat de mobiele telefoons (artefacten), zijn dat de gebruikers van de telefoons (lichamen) of is dat het getuige zijn of plegen van de moord (acties)? De mobiele telefoons zouden opgevat kunnen worden als het surveillanceobject, omdat de politie hierover gegevens inwint. ‘Mobiele telefoons’ is dan het antwoord op de vraag ‘wat beweegt er?’. Dit antwoord valt echter af als je bedenkt dat de politie eigenlijk niet geïnteresseerd is in die telefoons, maar in de mensen die zich rond de plaats en het tijdstip van de moord bewogen. Om die reden zouden de telefoongebruikers als surveillanceobjecten kunnen worden gezien, ware het niet dat de politie in de beschreven situatie geen gegevens over lichamen inwint (zoals wel het geval zou zijn bij bijvoorbeeld cameraopnames). De derde optie, de actie zelf, zou ook opgevat kunnen worden als het surveillanceobject, als je ervan uitgaat dat het doel van de surveillance is om informatie te verkrijgen over de gepleegde moord. Voor een begrip van mobiliteitssurveillance is het van belang om helder te krijgen wat bedoeld wordt met het surveillanceobject. Het onderscheid tussen gegevens en informatie helpt om dit duidelijker te krijgen.

Brimicombe en Li zetten de relatie tussen data¹⁷ en informatie kernachtig uiteen:

‘A *datum* is a fact, often in the form of measurement or as an indication that something is perceived to exist or has occurred. *Data* are thus collections of facts – the building blocks of information, evidence and knowledge. *Information* is something about which we are informed (have communicated to us – or become known to ourselves) usually as a result of analysing or interpreting data. Information is often (should be) the basis for rational decision making.’

(Brimicombe en Li, 2009: 137)

Uit bovenstaande valt af te leiden dat het van de specifieke context afhangt welke informatie uit bepaalde data naar voren komt en welke besluiten vervolgens genomen worden. Zo kunnen locatie- en tijdsgegevens van OV-chipkaarten door een koppeling aan persoonsgegevens uit klantbestanden leiden tot informatie over reisgedrag van NS-klanten en een besluit van de NS bepaalde klanten informatie toe te sturen.

¹⁷ Ik gebruik de aanduidingen data en gegevens als synoniemen van elkaar.

‘Het gebruik van de OV-chipkaart levert ons meer inzicht in het gebruik van onze treinen en producten. Afgeleide reisgegevens, zoals reisfrequentie, voorkeurstations en -trajecten, de verstreken tijd sinds uw laatst gemaakte reis en of u binnen of buiten de spits reist, gebruiken wij voor relatiebeheer en om u te informeren over voor u relevante diensten en producten.’ (NS, 2010)

Dezelfde data kunnen in een andere context, zoals die van opsporingsonderzoek door de politie, leiden tot andere informatie en een ander besluit. Zo heeft de Rotterdamse politie met behulp van OV-chipkaartgegevens getuigen van een aanranding opgespoord (Van 't Hof, Van Est en Daemen, 2010). Wat zegt het onderscheid tussen gegevens en informatie dan over de aard van het surveillanceobject?

De vraag ‘Wat beweegt er?’ lijkt op drie surveillanceniveaus een antwoord te kunnen krijgen. Het eerste niveau is dat van de gegevensinwinning/waarneming. Op dit niveau wordt het object beschreven, dat feitelijk wordt gelokaliseerd. In het eerder beschreven voorbeeld van de moordzaak, zijn dat mobiele telefoons en in het voorbeeld van de NS zijn dat ov-chipkaarten. Het tweede niveau is dat van gegevenskoppeling. Op dit niveau wordt het object beschreven waarvan reeds in databestanden aanwezige gegevens gekoppeld worden aan de gegevens van het eerste niveau. In het eerste voorbeeld zijn dat de personen die in de bestanden van telecomproviders geregistreerd staan als gebruikers van de gelokaliseerde telefoonnummers. In het tweede voorbeeld zijn dat de personen die volgens het NS-klientenbestand bij de betreffende OV-chipkaarten horen. Het derde niveau waarop het surveillanceobject beschreven kan worden is dat van gegevensanalyse/informatieverkrijging. Op dit niveau betreft het object één of meerdere, mogelijk elkaar overlappende categorieën van mensen die worden gespecificeerd aan de hand van de beleidscontext waarin de gegevens van de eerste twee niveaus worden geïnterpreteerd.¹⁸ In het eerste voorbeeld gaat het dan om relevante categorieën mensen voor het oplossen van een moordzaak, zoals de dader(s) en getuige(n). Het tweede voorbeeld liet al zien dat dezelfde gegevens in verschillende contexten tot andere informatie kan leiden. Zo is het surveillanceobject in de NS-context te definiëren aan de hand van categorieën als ‘frequente reiziger’ en ‘frequent gebruiker van station X’ en in de politiecontext als ‘getuige’. Hoe verhouden de drie niveaus waarop het surveillanceobject beschreven kan worden zich nu tot de drie objectcategorieën van Bennett en Regan (2004: 451)? Deze lijken niet op alle niveaus van toepassing te zijn. In onderstaand schema wordt dit duidelijk.

¹⁸ Hiermee wil ik niet suggereren dat het vaststellen van het surveillanceobject op het niveau van informatieverkrijging in de praktijk van mobiliteitssurveillance altijd volgt op de definities op het eerste en tweede niveau. Het omgekeerde kan ook het geval zijn.

Surveillanceniveau	Object-categorie	Voorbeeld 1 Moordzaak	Voorbeeld 2 Reisgedrag
Gegevensinwinning/ Waarneming	– Artefact – Lichaam	Mobiele telefoon	OV-chipkaart
Gegevenskoppeling	– Lichaam	Mobiele telefoon-gebruiker	OV-chipkaart-gebruiker
Gegevensanalyse / Informatieverkrijging	– Lichaam – Actie	Getuige / verdachte	Frequente reiziger

Tabel 1: Het surveillanceobject: wat beweegt er?

De tabel laat zien dat artefacten zoals mobiele telefoons, chipkaarten of auto's alleen op het niveau van gegevensinwinning/waarneming het object van surveillance zullen zijn. Personen daarentegen zijn op alle drie de niveaus een relevante categorie. Personen kunnen bijvoorbeeld direct waargenomen worden door camera's. Vervolgens kunnen reeds geregistreerde gegevens over personen, zoals naam of leeftijd, gekoppeld worden aan de gegevens die bij de waarneming zijn gegenereerd. Op dit niveau wordt de (deel)identiteit van het waargenomen object vastgesteld. Tenslotte kunnen personen op het niveau van gegevensanalyse het object van surveillance zijn. Dit is het geval wanneer de surveillant tot doel heeft om de mobiliteit van een bepaalde persoon of een groep personen met bepaalde kenmerken in beeld te brengen. Als het doel niet zozeer is om de mobiliteit van mensen met bepaalde persoonskenmerken in beeld te brengen, maar als mensen geselecteerd worden op basis van de handelingen die ze verrichten, dan is de actie het surveillanceobject. Dat met het vaststellen van het surveillanceobject persoonsgegevens gemoeid zijn, is evident. Om welk type persoonsgegevens het gaat, hangt echter af van zowel het surveillanceniveau als de objectcategorie. Hier kom ik in paragraaf 3.2 op terug.

2.2.2 Dimensie 2: de beweging zelf

De tweede dimensie van mobiliteit betreft de beweging zelf.

'This is a more complicated concept because one is trying to capture something that is by definition in motion, either, as Clarke states, from place A to place B, or from time 1 to time 2, or in relation to the movement of the earth. Thus we propose that mobility should not be viewed in terms of static categories but instead is more appropriately regarded as a continuum.'

(Bennett en Regan, 2004: 451)

Door mobiliteit als een continuüm te beschouwen, sluiten Bennett en Regan aan bij Manuel Castells' theorievorming rondom de 'space of flows': 'our society is constructed around flows: flows of capital, of information, of technology, flows of organizational interaction, of images, sounds, and symbols' (Castells, 2000: 442). Met de vernuftige uitwerking van zijn stromenland als 'the material organization of time-sharing social practices that work through flows' (Ibid.) werpt Castells licht op de maatschappelijke betekenis van plaats en tijd. De logica van stromenland zegt iets over plaats en tijd, maar andersom zijn plaats en tijd de materiële aanknopingspunten om stromen inzichtelijk te maken. Ondanks de terughoudendheid van Bennett en Regan lijkt een nadere informatietechnologische specificatie van de tweede dimensie van mobiliteit, de beweging zelf, mij wel degelijk mogelijk en zinvol. Feitelijk geven zij hier zelf al een aanzet toe door de dimensies van plaats en tijd te noemen. Bij ruimtelijke mobiliteit gaat het net als bij sociale mobiliteit om beweging, verschuiving en verandering, maar dan met betrekking tot de plaats en tijd van mensen.

Beweging in de dimensies van plaats en tijd heet ook wel translocatie of verplaatsing. Mobiliteit heeft altijd hiermee of in ieder geval met de mogelijkheid hiertoe te maken. Als ik me van locatie A naar locatie B verplaats, ben ik mobiel, maar dit hoeft ik niet daadwerkelijk te doen om als zodanig gekwalificeerd te worden. Het feit dat ik tot deze translocatie in staat ben, maakt mij al mobiel en daarmee een object voor mobiliteitssurveillance, zo bevestigt Soenens (2006: 35): 'Related to mobility, "mobile" refers to something that is able to move, so it is the opposite of "static". De dubbele betekenis van 'mobiel' als 'zich verplaatsend' en 'in staat zijn tot verplaatsing' komt ook terug in Roger Clarkes veel geciteerde conceptualisering van de term 'mobile'. Clarke (2003) noemt vier kenmerken, waarvan een apparaat er één of meerdere kan hebben, waardoor mensen dit als mobiel zouden bestempelen. Het eerste kenmerk betreft de *mogelijkheid tot beweging in plaats en tijd*: 'devices may be "mobile" in the limited sense of *being able* to be in a different location at any given time from that in which they were at one or more previous times'. Ten tweede kan de term mobiel duiden op *onzekerheid over de huidige locatie*: 'a device might be in any location from which transmission to another device is possible'. Een derde betekenis van 'mobiel' is het *in beweging zijn*: 'a further interpretation of "mobile" is in the more substantial sense of currently moving relative to the earth's surface, but nonetheless capable of sustaining data transmission, e.g. as a passenger in a plane, a train, a taxi, or a car, or, less safely, as the driver of a car'. Ten vierde kan een apparaat volgens Clarke mobiel genoemd worden als het *gemakkelijk verplaatsbaar* is: 'yet another sense of the term "mobile" is to refer to devices that are designed to be easily and conveniently portable, and to rely on wireless transmission, possibly to the extent that they do not support cable-based connections'. Het moge duidelijk zijn dat 'mobiel' meerdere dingen kan betekenen. Tegelijkertijd staan de vier kenmerken van Clarke niet los van elkaar. Het eerste kenmerk, de mogelijkheid tot beweging in plaats en tijd, is een

voorwaarde voor de overige drie kenmerken. Als iets niet *kan* bewegen, zal het nooit gekenmerkt worden als dat het overal kan zijn, in beweging is of gemakkelijk verplaatsbaar is. De essentie van mobiliteit is dan ook de *mogelijkheid* tot bewegen van een object in de dimensies van plaats en tijd. Publieke mobiliteitssurveillance heeft daarom net zo goed betrekking op stilstaande als zich verplaatsende personen. Of mensen zich verplaatsen en zo ja, waar en wanneer ze dit doen, is typisch informatie die met mobiliteitssurveillance verkregen kan worden.

3 Mobiliteitsgegevens: object, plaats en tijd

3.1 Inleiding

In de vorige paragraaf is naar voren gekomen dat mobiliteit conform Bennett en Regan (2004) twee dimensies heeft: het surveillanceobject dat (mogelijk) beweegt (artefact, lichaam en/of actie) en de beweging zelf. De gegevens die verzameld en verwerkt worden bij publieke mobiliteitssurveillance, de mobiliteitsgegevens, beslaan dan ook beide dimensies. Gegevens over het surveillanceobject geven antwoord op de vraag ‘Wie of wat is het surveillanceobject?’. Gegevens over de beweging zelf betreffen gegevens van plaats (locatiedata) en gegevens van tijd (temporele data).



Figuur 1: Mobiliteitsgegevens

In alle drie de gegevenstypen is variatie mogelijk. In deze paragraaf behandel ik achtereenvolgens object-, plaats- en tijdsgegevens.

3.2 Objectgegevens: wie/wat...?

In paragraaf 2.2.1 heb ik de drie objectcategorieën artefact, lichaam en actie geïntroduceerd en op hoofdlijnen beschreven. Deze categorieën helpen een antwoord te geven op de vraag: ‘Wie/wat is ergens op een bepaald moment?’ Om wat voor gegevens gaat het nu in ieder van deze categorieën?

Artefact

De artefacten die relevant zijn voor publieke mobiliteitssurveillance hebben vrijwel altijd een uniek kenmerk aan de hand waarvan ze herkend kunnen worden. Zo heeft een motorvoertuig een kenteken, een ov-chipkaart een chipnummer en de SIM-kaart¹⁹ in een mobiele telefoon een uniek nummer. Dit unieke kenmerk wordt echter niet altijd vastgelegd. In sommige beleidssituaties volstaat het om te weten hoeveel artefacten ergens zijn. Dan gaat het er niet zozeer om precies te weten welke dit dan precies zijn.

Lichaam

Ook in deze objectcategorie kunnen de gegevens variëren in specificiteit. Er kan sprake zijn van unieke identiteitskenmerken zoals naam, burgerservicenummer en gelaatsafmetingen, maar ook van groepskenmerken zoals leeftijd en sekse. Daarnaast is het mogelijk de aanwezigheid van één of meerdere personen anoniem te registreren. Het antwoord op de vraag ‘Wie waren op locatie x?’ zou dan bijvoorbeeld beantwoord kunnen worden met ‘tien personen’.

Actie

Bij actiegegevens gaat het om iemands situationele identiteit. Deze situationele identiteit hangt volledig af van de (vermoedelijke) handeling(en) die iemand verricht en de beleidsrelevantie daarvan. Gaat iemand op tijdstip t en locatie x inbreken? Heeft iemand op tijdstip u en locatie y autogereden? Inbreken en autorijden zijn dan de objectgegevens die vastgesteld worden. De mobiliteitsinformatie die hiermee gegenereerd kan worden is dat er vermoedelijk een inbraak plaatsvindt op tijdstip t en locatie x. Welke persoon hieraan gekoppeld kan worden is een ander type objectgegeven, namelijk van lichaam.

¹⁹ SIM staat voor Subscriber Identity Module.

Objectcategorie	Vorm	Voorbeelden
Artefact	Apparaatgegevens	SIM-kaartnummer; chipkaartnummer
Lichaam	(Geaggregeerde) persoonsgegevens	NAW-gegevens; leeftijd; sekse
Actie	Situationele identiteit	Automobilist; gewonde; getuige

Tabel 2: Objectcategorieën

3.3 Plaatsgegevens: waar...?

De betekenis van plaats is niet zonder meer eenduidig. Als er wordt gevraagd naar een plaats, is dat altijd de ‘waar’-vraag in relatie tot iets of iemand. Waar is meneer Jansen? Waar is de auto met kenteken xx-yy-11? Maar wat voor antwoorden zijn er nu mogelijk op een vraag naar plaats? Wat kan ‘waar’ zijn? ‘Waar’ verwijst doorgaans naar een locatie in de fysieke wereld (Küpper, 2005: 17), in tegenstelling tot de virtuele wereld van het world wide web. Dit type informatie wordt ook wel geo-informatie genoemd: ‘all information which is linked, in one way or another, to a place on the surface of the earth’ (Bregt, 1999). Küpper (2005: 18) onderscheidt drie locatie-categorieën voor de fysieke wereld die ieder een andere manier aangeven om te zeggen waar iets of iemand zich bevindt op het aardoppervlak: ruimtelijke, netwerk- en beschrijvende locaties.

Ruimtelijke locaties

‘Waar’ verwijst in deze categorie naar één uniek punt, ook wel positie genoemd, die doorgaans wordt weergegeven met twee- of driedimensionale coördinaten die verwijzen naar de assen of dimensies waarin wetenschappers de Aarde hebben ingedeeld. Mijn ruimtelijke locatie kan bijvoorbeeld weergegeven worden als H 55m N 51.5629° O 5.0472°. Ruimtelijke locaties zijn met name belangrijk voor professioneel gebruik zoals in het leger en de scheepvaart, omdat men hierbij afhankelijk is van een hoge precisie en accuraatheid van locatie-informatie.

Netwerkllocaties

‘Waar’ wordt in deze categorie weergegeven volgens de topologie van een communicatienetwerk, zoals het GSM-netwerk of het internet. Een communicatienetwerk is dan het referentiesysteem om de locatie van een apparaat uit te drukken. Netwerkadressen bevatten routinginformatie waarmee nummers of andere identifiers aan een netwerkadres gekoppeld kunnen worden. In een mobiel communicatienetwerk hangt de netwerkllocatie bijvoorbeeld af van het basisstation waar een mobiel apparaat

mee is verbonden. De netwerklocatie is essentieel voor de dienstverlening in het betreffende communicatienetwerk. Zo kan ik niet mobiel bellen zonder dat mijn netwerkprovider weet waar mijn telefoon zich bevindt in het netwerk.

Beschrijvende locaties



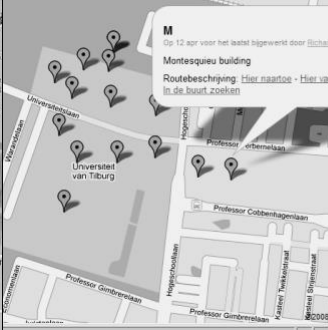
‘Waar’ krijgt in deze categorie de vorm van een beschrijving van een plaats, zoals deze gegeven wordt in het dagelijks taalgebruik. Een zekere locatie kan weergegeven worden met uitspraken als:

1. ‘Laten we elkaar *bij 't Haantje* ontmoeten.’
2. ‘We zien elkaar aan de Daalseweg nummer 19.’
3. ‘Vanavond in dat café naast Station Oost.’

Naast deze drie beschrijvingen bestaan nog talloze andere talige uitingen om deze locatie aan te duiden, waarbij gevarieerd kan worden in de kenmerken en details die worden genoemd. Wat alle mogelijke beschrijvende locaties gemeen hebben is dat ze verwijzen naar geografische objecten. Dit kunnen natuurlijke objecten zijn, zoals bergen, rivieren en bossen, maar ook door de mens gecreëerde objecten, zoals grenzen, steden en straten. De drie voorbeelduitspraken verwijzen ieder op een andere manier naar hetzelfde gebouw. Een belangrijke factor in de keuze voor een bepaalde beschrijving van een locatie is de veronderstelde voorkennis bij de ontvanger van de boodschap. Zo gaat de zender er in alle drie de gevallen van uit dat de ontvanger weet dat de locatie in de stad Nijmegen is, maar wordt in voorbeeld 1 en 3 specifieke lokale kennis verondersteld waar dit in voorbeeld 2 in mindere mate het geval is.

Aangezien geslaagde communicatie over het ‘waar’ van een persoon x één van de basiselementen is van publieke mobiliteitssurveillance, is het van belang om zich bewust te zijn van mogelijke verschillen in beschrijvende locaties. Geografische informatiesystemen (GIS) zijn uitstekende hulpmiddelen om communicatie te realiseren over ruimtelijke, netwerk- en beschrijvende locaties. Het onderwerp GIS komt verder aan bod in paragraaf 5.3.

Figuur 2 laat zien waar ik mij bevind met mogelijke visuele weergaven van de ruimtelijke, netwerk-, en beschrijvende locatie.

Ruimtelijke locatie b.v. GPS-coördinaten	Netwerkllocatie b.v. Plaats in GSM-netwerk via Cell-ID	Beschrijvende locatie b.v. De naam van het gebouw van de Tilburg Law School
 <p>Bron: www.gpscoordinaten.nl</p>	 <p>Bron: www.antenneregister.nl</p>	 <p>Bron: maps.google.nl</p>

Figuur 2: Mijn locatie op drie manieren

Het antwoord op de vraag ‘Waar is persoon x?’ kan dus verschillende vormen aannemen. In onderstaande tabel staan de belangrijkste kenmerken van de drie categorieën van locatieaanduidingen op een rijtje.

Locatiecategorie	Vorm	Voorbeelden
Ruimtelijk	Coördinaten	Punt in een cartesiaans (X,Y,Z) of ellipsoïde (N; O) coördinatensysteem ²⁰
Netwerk	Cell-topologie	IP-adres; plaats in GSM-netwerk
Beschrijvend	Geografische verwijzing	Adres; naam van gebouw/park/stad

Tabel 3: Locatiecategorieën

Van welke locatiecategorie sprake is in een bepaalde praktijk van publieke mobiliteitssurveillance hangt af van het palet aan actoren en technologieën dat hierbij betrokken kan zijn, waarover meer in de paragrafen 4 en 5.

²⁰ Zie Küpper (2005: 20-23) voor een gedetailleerde beschrijving van beide coördinatensystemen.

3.4 Tijdsgegevens: wanneer...?

Voor publieke mobiliteitssurveillance is het niet alleen essentieel om te bepalen waar iemand is, maar ook *wanneer* iemand ergens is. Behalve de vraag ‘Waar *is* persoon x?’, zijn de vragen ‘Waar *was* persoon x?’ en ‘Waar *zal* persoon x *zijn*?’ ook relevant. Ik maak een onderscheid in mobiliteitsgegevens over het heden, het verleden en de toekomst.

Heden

Mobiliteitsgegevens over het heden betreffen het hier en nu. In realtime worden gegevens ingewonnen over ruimtelijke, netwerk- of beschrijvende locaties om zicht te krijgen op een actuele situatie. De vraag is echter: wat is actueel? Op het moment dat er gegevens zijn over iemands actuele locatie kan deze al weer veranderd zijn. Vanuit technisch perspectief is de latentie van gegevens hierbij een belangrijk aspect: ‘*Latency* refers to the time period between a position request and the subsequent delivery of a position fix’ (Küpper 2005: 126). Latentie wordt beïnvloed door de gebruikte meetmethode en de actuele omstandigheden, zoals belasting van een netwerk of bewolking. Wanneer iemand wordt gevolgd over een langere tijdsperiode maakt het ook uit of het de eerste of een latere meting betreft in een serie van metingen. De eerste plaatsbepaling duurt meestal het langst, omdat de benodigde technologie dan nog moet worden ingeschakeld. Daarom is de *Time To First Fix (TTFF)*, de tijd die nodig is voor de eerste meting, een belangrijke indicator. De TTFF is in de huidige applicaties een kwestie van seconden (Küpper, 2005: 126). Technisch gezien is er dus altijd een beperking op het begrip ‘actueel’. Uitgaand van de definitie van het begrip latentie is er sprake van gegevens over het heden als er aansluitend aan het verzoek om mobiliteitsinformatie een plaatsbepaling plaatsvindt. Ik wil weten waar iemand zich op dit moment bevindt en krijg binnen een paar seconden de benodigde gegevens.

Verleden

Bij mobiliteitsgegevens over het verleden heeft de plaatsbepaling al vóór het informatieverzoek plaatsgevonden. Van persoon x is de (ruimtelijke, netwerk- en/of beschrijvende) locatie vastgesteld en nu wil ik graag weten welke deze was. Om deze gegevens uit het verleden te kunnen verkrijgen, moet er in het heden iets extra’s gebeuren met de realtime-gegevens. Op het moment dat realtime-gegevens worden opgeslagen in een database verworden ze tot historische gegevens. Tijd kan in absolute of relatieve termen worden opgeslagen (Brimicombe en Li, 2009: 255). Absolute tijd betekent een datum- en tijdstempel voor ieder locatiegegeven. Dan kan ik op tijdstip (t) in mijn database bekijken waar persoon x op tijdstip (t-1; t-2...t-z) was. Bij relatieve tijd gaat het om de verstreken tijd gerekend vanaf een arbitrair startpunt. Over persoon

x kan bijvoorbeeld (van meerdere gelegenheden) opgeslagen worden hoe lang zijn reistijd was van locatie A naar locatie B.

Toekomst

Technisch gezien kunnen (nog) geen toekomstige mobiliteitsgegevens ingewonnen worden. Er zijn geen detectiemethoden beschikbaar die met 100% zekerheid kunnen bepalen waar persoon x zich op tijdstip (t+1 seconde/minuut/dag/week of jaar) zal bevinden. Dat toekomstige data niet beschikbaar zijn, betekent echter niet dat er geen informatie over de toekomst gegenereerd kan worden. Aan de hand van de gegevens die wel beschikbaar zijn, die uit het verleden, kan de toekomst wel berekend worden. Dit noemt men voorspellen. Net als bij weersvoorspellingen zijn mobiliteitsvoorspellingen nauwkeuriger naarmate ze dichter bij het heden liggen. Een groot verschil met weersvoorspellingen is dat het bij mobiliteit gaat om bewegingen van mensen en niet natuurverschijnselen. Mobiliteitsvoorspellingen gaan dan ook om toekomstig menselijk gedrag, dat afhankelijk is van meer dan natuurwetten alleen.

Het antwoord op de vraag ‘Wanneer is persoon x?’ kan dus verschillende inhouden en vormen aannemen. In onderstaande tabel staan de belangrijkste kenmerken van de drie tijds categorieën op een rijtje.

Tijds categorie	Vorm	Voorbeelden
Heden	Realtime ingewonnen gegevens	Actuele locatie van tbs-veroordeelden met enkelband; locatie van 112-noodoproep
Verleden	Opgeslagen gegevens	Historische wegverkeersgegevens; ov-chipkaart reistijdgegevens
Toekomst	Gecalculeerde gegevens	Verwachte filevorming; terrorismedreiging

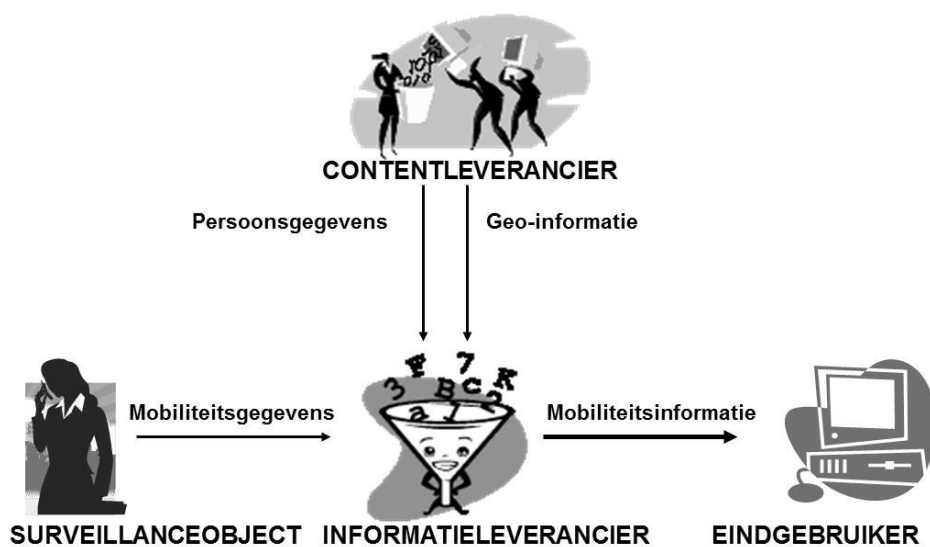
Tabel 4: Tijds categorieën

4 Actoren en gegevensstromen in de totstandkoming van mobiliteitsinformatie

4.1 De gegevensketen voor mobiliteitsinformatie

De vorige paragraaf heeft duidelijk gemaakt dat mobiliteitsinformatie aspecten van plaats, tijd en object in zich heeft. Deze inhoudelijke kwalificatie van mobiliteitsinformatie zegt niets over het proces waarlangs de informatie tot stand komt. In deze paragraaf besteed ik aandacht aan de actoren die betrokken zijn bij de totstandkoming

en het gebruik van mobiliteitsinformatie. Een manier om te kijken naar het proces van inwinning, koppeling en interpretatie van mobiliteitsgegevens is door de betrokken actoren te benoemen. Een actor dient hierbij opgevat te worden als een individu, een organisatie of onderneming die diensten aanbiedt aan, of afneemt van andere actoren, of beide. Afgeleid van de supply chain voor Location-Based Services (LBS) van Küpper (2005: 250) geeft figuur 3 een actorbenadering van de totstandkoming van mobiliteitsinformatie.



Figuur 3: Actoren en gegevensstromen voor mobiliteitsinformatie

Dit model wordt hier toegelicht aan de hand van een bekend voorbeeld van het gebruik van mobiliteitsinformatie in het openbaar bestuur. In maart 2006 vraagt de Politie Nijmegen locatiegegevens van mobiele telefoons op in de hoop mogelijke getuigen te vinden in de moordzaak van de activist Louis Sévèke. 3000 mensen ontvangen een sms van de politie met het verzoek zich te melden als ze informatie hebben over de moord (Nu.nl, 2006). Deze mensen zijn niet geselecteerd, omdat ze in de buurt van de plaats delict wonen of omdat ze het slachtoffer kennen. De enige reden waarom ze worden benaderd is hun locatie, dat wil zeggen, de locatie van hun mobiele telefoons ten tijde van de moord. De locatie- en tijdsgegevens zijn bewaard door de telecomproviders en worden op verzoek van de autoriteiten opgevraagd. Hoe past dit verhaal nu in het bovenstaande model?

Surveillanceobject

Dit is het mobiele individu dat gelokaliseerd, gevolgd of waargenomen moet worden. De lokalisatie kan plaatsvinden door mobiele apparatuur die het individu bij zich draagt, zoals een GSM, GPS-ontvanger of chippas, maar ook door technologie zoals nummerplaatherkenning of bewakingscamera's waarmee het passerend individu wordt geregistreerd. Ruwe locatiegegevens zoals coördinaten of cell-topologische gegevens gaan samen met tijdsgegevens en objectkenmerken naar de informatieleverancier voor verdere verwerking. In het voorbeeld zijn de 3000 benaderde burgers, of eigenlijk de 3000 telefoons die in het door de politie gedefinieerde gebied aanwezig zijn, te beschouwen als objecten van publieke mobiliteitssurveillance.

Contentleverancier

Deze actor is beheerder van databases met gegevens die relevant kunnen zijn voor een bepaalde vraag naar mobiliteitsinformatie. Het gaat hierbij om gegevens zoals kaartmateriaal, aanvullende geografische data of persoonsgegevens over het object. Zodoende ondersteunt de contentleverancier de informatieleverancier door het aanleveren van gegevens die de informatieleverancier nodig heeft om de juiste informatie te kunnen genereren. In het voorbeeld vervullen de betrokken telecomproviders de rol van contentleveranciers door bij de gelokaliseerde telefoons horende persoonsgegevens in de vorm van telefoonnummers aan te leveren.

Informatieleverancier

Deze actor, wiens rol veelal wordt vervuld door zich daartoe gespecialiseerde bedrijven, heeft een centrale rol in de gegevensketen. Hij verzamelt locatiegegevens van één of meerdere objecten, voert ruimtelijke analyses uit, maakt combinaties met andere (geografische) data, verkregen van de contentleverancier, en stuurt de uiteindelijke applicatiedata door naar de eindgebruiker. Aldus vertaalt en verrijkt de informatieleverancier ruwe mobiliteitsgegevens naar voor de gebruiker betekenisvolle mobiliteitsinformatie. In het voorbeeld blijken de telecomproviders naast de rol van contentleverancier ook die van informatieleverancier te vervullen. De uiteindelijk opgeleverde mobiliteitsinformatie bestaat uit een lijst met telefoonnummers (persoonsgegevens) waarvan de bijbehorende SIM-kaarten en toestellen rond het tijdstip van de moord in het gebied aanwezig waren (mobiliteitsgegevens).

Eindgebruiker

Dit is de actor die de mobiliteitsinformatie tot zich neemt via bijvoorbeeld een mobiele telefoon, PDA of PC. In de Sévèke-zaak kan de Nijmeegse politie gezien worden als

eindgebruiker, als afnemer van de informatiedienst. De verkregen mobiliteitsinformatie stelt de politie vervolgens in staat om actie te ondernemen door sms'jes te sturen aan de geselecteerde burgers.

4.2 Rollen van overheid en burger in de totstandkoming van mobiliteitsinformatie

Overheid en burger kunnen in de gegevensketen verschillende rollen aannemen. De overheid kan twee verschillende, elkaar niet uitsluitende rollen vervullen in de gegevensketen: contentleverancier en eindgebruiker. Burgers kunnen bij het realiseren van mobiliteitsinformatie meerdere rollen tegelijkertijd spelen. Mogelijke rollen zijn die van surveillanceobject, contentleverancier en eindgebruiker. Rondom combinaties van deze rollen zijn verschillende scenario's weer te geven.

Het voorbeeld van de Sévèke-zaak toont aan dat burgers de rol van surveillanceobject kunnen hebben en de overheid die van eindgebruiker. In dit scenario is de overheid dominant. Een extra variant op dit scenario is te zien wanneer de overheid naast de rol van eindgebruiker ook die van contentleverancier vervult, bijvoorbeeld door zelf persoonsgegevens over de subjecten aan te bieden. Een voorbeeld hiervan is het elektronisch volgsysteem voor tbs'ers op proefverlof door middel van GPS-enkelbanden (Van Gestel, Van der Knaap en Hendriks, 2006; Miedema en Post, 2006). Hierbij beschikken politie en justitie zelf over de persoonsgegevens om een bepaalde enkelband met de identiteit van een zekere tbs-veroordeelde in verband te brengen.

In een ander scenario heeft de burger een iets dominantere positie. Wederom is deze het surveillanceobject, maar vervult tevens de rol van contentleverancier. Ook hier zijn twee varianten denkbaar. In de eerste variant is de burger de exclusieve contentleverancier. Hier is bijvoorbeeld sprake van indien een burger meewerkt aan een analyse van mobiliteit in een stad op basis van mobiele telefoongegevens en hiertoe van tevoren persoonlijke informatie afstaat. Essentieel hierbij is dat de burger alleen als contentleverancier beschouwd kan worden als hij expliciet toestemming heeft gegeven voor het gebruik van de persoonsgegevens voor die specifieke toepassing. Indien dezelfde persoonsgegevens later zonder toestemming in een andere beleidssituatie gebruikt zouden worden, wordt de rol van contentleverancier niet vervuld door die burger, maar door de instantie die de gegevens op dat moment voor die specifieke toepassing afstaat. In de tweede variant is de invloed van de overheid toch weer iets groter doordat deze ook als contentleverancier fungeert. Dit is bijvoorbeeld het geval wanneer de overheid geo-informatie aanlevert in de vorm van kaartmateriaal, waardoor deze controle heeft over de weergave van grenzen en andere belangrijke informatie in de omgeving van de surveillanceobjecten.

Het is ook denkbaar dat de burger tegelijkertijd surveillanceobject en eindgebruiker is van mobiliteitsinformatie. De burger wordt gelokaliseerd, waarna de mobiliteitsgegevens worden verwerkt en verrijkt door andere partijen om uiteindelijk gebruikt te worden door diezelfde burger. Dit komt voor in navigatietoepassingen, waarbij de burger wordt gelokaliseerd door middel van GPS en vervolgens op basis hiervan visuele en auditieve aanwijzingen krijgt voor de te volgen route. Het behoort ook tot de mogelijkheden dat in de uiteindelijke mobiliteitsinformatie gegevens van andere burgers worden verwerkt, bijvoorbeeld door realtime file-informatie weer te geven op basis van een clustering van mobiele telefoons op de weg.²¹ De overheid zou in dit scenario de rol van contentleverancier kunnen spelen en daardoor invloed uit kunnen oefenen op de informatieoutput. In het geval van navigatiesystemen bijvoorbeeld kan de overheid dit doen door data aan te leveren met snelheidslimieten of routes waar de burger langs wordt gestuurd.

5 Technologieën voor mobiliteitssurveillance

5.1 Waarnemen en context genereren

Een scala aan technologieën is betrokken bij de totstandkoming van mobiliteitsinformatie. Eerder in dit hoofdstuk is duidelijk geworden dat dit proces in drie fases verloopt van achtereenvolgens gegevensinwinning/waarneming, gegevenskoppeling en gegevensanalyse/informatieverkrijging. In de nu volgende bespreking behandel ik twee groepen technologieën die deze drie fases faciliteren: plaatsbepalingstechnologieën en geografische informatiesystemen (GIS).

Plaatsbepalingstechnologieën zorgen door het genereren van locatie- en tijdsgegevens voor de waarneming van het surveillanceobject. De koppeling met persoonsgegevens en de contextualisering in de geografisch-bestuurlijke werkelijkheid komt vervolgens in een GIS tot stand. De netwerktechnologie die nodig is voor het datatransport tussen de plaatsbepalingstechnologie en het GIS bespreek ik niet als aparte categorie, maar komt waar nodig aan bod om de werking van de andere technologieën te verduidelijken.

²¹ Dit voorbeeld verwijst naar de HD Traffic dienst die TomTom sinds 2007 in samenwerking met Vodafone aanbiedt. Realtime locatiegegevens van Vodafone abonnees worden weergegeven in TomTom navigatiesystemen.

5.2 Plaatsbepalingstechnologieën

5.2.1 *Categorisering van plaatsbepalingstechnologieën*

In de literatuur bestaan diverse categorisering van plaatsbepalingstechnologieën (Brimicombe en Li, 2009; Küpper, 2005; Meints en Royer, 2007; Mountain en Raper, 2001; Raper et al., 2007). Zo onderscheiden Brimicombe en Li (2009) technologieën waarbij de plaatsbepaling tot stand komt in een apparaat (device-based), netwerk (network-based) of een combinatie van beide (hybrid solutions). Een nadeel van deze categorisering is dat deze gebaseerd is op het idee van ‘fixing the location of users through their mobile device’ (Brimicombe en Li, 2009: 169) en daarmee weinig ruimte laat voor optische of biometrische technologieën. De auteurs lijken zelf de beperking van de door hen voorgestelde hoofdcategorisering in te zien, aangezien ze in een aparte paragraaf nog een categorie ten tonele voeren: ‘short range positioning technologies’. Onder deze noemer presenteren de auteurs technologieën als WiFi en infrarood. Evenals Brimicombe en Li (2009: 171) ben ik mij ervan bewust dat de hier gepresenteerde classificatie één van de vele mogelijke indelingen betreft: ‘They can also be differentiated as to whether they are integrated or stand-alone positioning structures, and again depending on whether they are satellite-based, network-based (cellular) or indoor infrastructures’.

In onderstaande bespreking maak ik gebruik van de onderverdeling van Meints en Royer (2007: 16), die evenals dit proefschrift niet primair voor een technisch onderlegd publiek is geschreven. Hun onderverdeling werk ik uit aan de hand van de technische specificaties van Brimicombe en Li (2009). Meints en Royer maken gebruik van zes categorieën. Ten eerste zijn dat satellietssystemen zoals het Amerikaanse GPS-systeem en het in ontwikkeling zijnde Europese GALILEO-systeem. Een tweede belangrijke groep vormen de cell-gebaseerde mobiele communicatienetwerken (GSM; UMTS). Als derde komen overige draadloze technologieën in beeld. Hierbij valt onder andere te denken aan RFID (Radio Frequency Identification), Bluetooth en WiFi. Ten vierde gaat het om systemen die werken op basis van sensoren, zoals biometrische systemen, optische sensoren en passieve infrarood systemen. Ten vijfde worden hier chipkaartsystemen genoemd. Het gaat dan om zaken als bankautomaten en toegangspassen voor gebouwen. De genoemde technologieën verschillen wat betreft precisie, de aard van de verzamelde data, afstand tot de te lokaliseren persoon, en of ze vaste of mobiele sensoren hebben. In de zesde categorie, de hybride technologieën, kan door een combinatie van verschillende plaatsbepalingstechnologieën de precisie en beschikbaarheid van de gegenereerde mobiliteitsinformatie worden vergroot. Een voorbeeld zijn mobiele telefoons met ingebouwde GPS, waardoor met grotere zekerheid kan worden bepaald waar de telefoongebruiker zich bevindt. Voor iedere

categorie illustreer ik het gebruik met een toepassing in het Nederlandse of buitenlandse openbaar bestuur. Er komen voorbeelden aan bod op de beleidsterreinen verkeer en vervoer, zorg en welzijn, openbare orde en veiligheid en ruimtelijke ordening.

5.2.2 Satellietssystemen

Plaatsbepaling door een Global Navigation Satellite System (GNSS) is apparaatgebaseerd (Brimicombe en Li, 2009: 172). Dit betekent dat het mobiele apparaat zijn positie bepaalt op basis van de signalen die het ontvangt. De locatieberekening vindt dus plaats in de satellietontvanger die het surveillanceobject bij zich draagt. Hiervoor is geen netwerkverbinding nodig. Het Amerikaanse Global Positioning System (GPS) is het meest bekende GNSS. Dit systeem heeft het Amerikaanse ministerie van Defensie oorspronkelijk ontworpen als defensiesysteem. De eerste satelliet werd in 1978 gelanceerd en werd in 1993 volledig operationeel. Op dat moment was het systeem echter nog niet volledig beschikbaar voor burgers: ‘Prior to May 2000, GPS signals from the satellites were selectively degraded to reduce the accuracies available for civilian use, and although this policy has been abandoned it could still be re-introduced’ (Brimicombe en Li, 2009: 173). De Europese ruimtevaartorganisatie ESA zinspeelt op deze angst in haar promotie van het Europese GALILEO-systeem: ‘Galileo is Europe’s own global navigation satellite system, providing a highly accurate, guaranteed global positioning service under civilian control’ (European Space Agency, 2012). Europa’s Galileo is volgens de ESA echter pas tegen 2020 volledig operationeel. Andere systemen zijn het Russische GLONASS-systeem en het Chinese BEIDOU-systeem. GLONASS is net als GPS volledig wereldwijd operationeel en BEIDOU werkt inmiddels in China en omliggende gebieden (Jin, 2013; Langley, 2012; Nu.nl, 2011). De basisprincipes van GPS, die gelijk zijn aan die van de overige GNSS, licht ik in het vervolg toe.

GPS werkt op basis van radiosignalen die een GPS-ontvanger binnenkrijgt van satellieten die op een afstand van ongeveer 20.200 kilometer rond de aarde cirkelen. De basisconstellatie bestaat uit 24 satellieten. Dit is het vereiste aantal om het gehele aardoppervlak te kunnen bedienen. De Amerikaanse luchtmacht, die verantwoordelijk is voor de werking van het systeem, heeft echter al een paar jaar 31 operationele satellieten en 3-4 inactieve reservesatellieten (NOAA, 2012). Het basisaantal van 24 satellieten garandeert dat er tenminste vier satellieten in zicht zijn vanaf ieder punt van de aarde. De geografische positie van een GPS-ontvanger wordt bepaald door de gemeten afstand tot een serie satellieten. Deze afstand wordt berekend door de reistijd van het radiosignaal van een satelliet te vermenigvuldigen met de lichtsnelheid. Een accurate tijdsbepaling is essentieel om accurate afstandsmetingen tussen een ontvanger

en satellieten te krijgen, en daarmee een accurate GPS-plaatsbepaling. De tijdsbepaling in de satellieten is zeer nauwkeurig, omdat deze ingebouwde atoomklokken hebben. De ingestelde tijd in GPS-ontvangers is echter minder nauwkeurig en kan daarom leiden tot meetfouten in de reistijd van het radiosignaal. Om een surveillanceobject te kunnen lokaliseren zijn in theorie in ieder geval drie, maar in de praktijk vier zichtbare satellieten vereist vanwege de mogelijke onnauwkeurigheid in de GPS-ontvanger.

Lokalisatie door GPS heeft een hoge nauwkeurigheid. Zo kunnen mobiele telefoons met ingebouwde GPS tot tussen ongeveer drie en vijftien meter nauwkeurig worden gelokaliseerd (Brimicombe en Li, 2009: 174). Dit niveau wordt niet in alle omgevingen gehaald: 'The accuracy may vary from rural areas to high-rise urban areas due to its need for a clear view of the sky and signals from three or four GPS satellites' (Ibid.).

In Nederland zijn enkele proeven gedaan met het uitrusten van tbs-veroordeelden met GPS-enkelbanden (Van Gestel et al., 2006; Miedema en Post, 2006) tijdens het proefverlof. Het blijkt echter geen waterdicht systeem te zijn, vanwege zowel de technische beperkingen van GPS binnenshuis en in drukke gebieden als opzettelijke verstoringen van de enkelband door bijvoorbeeld aluminiumfolie aan te brengen. Een andere GPS-toepassing op het gebied van openbare orde en veiligheid is het gebruik van mobiliteitsgegevens voor het opleggen van boetes. Snelheidsovertreders kunnen zo wellicht niet meer ontsnappen aan een boete. In de Verenigde Staten is al een rechtszaak geweest die laat zien dat dit een reële mogelijkheid is: 'James Turner v. American Rental Inc.' voor het Connecticut Superior Court (Brouwer, 2005). Turner huurde een auto en betaalde hiervoor met zijn creditcard. Diezelfde creditcard werd vervolgens geweigerd toen hij wilde betalen voor benzine, omdat zijn betalingslimiet was overschreden. Bij navraag bleek dat de verhuurmaatschappij GPS-apparatuur in zijn auto had geplaatst om zijn snelheid te meten. Bij iedere overtreding van de snelheidslimiet werd de bijbehorende boete alvast van zijn credit card betaald.

5.2.3 Cell-gebaseerde mobiele communicatienetwerken

In tegenstelling tot de beschreven satellietssystemen is het genereren van mobiliteitsgegevens bij mobiele telefonie een nevenfunctionaliteit (Cho, 2008). Deze nevenfunctionaliteit is in eerste instantie ontwikkeld als gevolg van veranderingen in de Amerikaanse telecommunicatiewet op het gebied van noodhulpverlening via 911, en later in de Europese regelgeving rondom 112 (Küpper, 2005: 8-9). Bij netwerkgebaseerde plaatsbepaling worden signalen gemeten tussen een mobiel apparaat en een aantal basisstations in een netwerk. De positie van het mobiele apparaat wordt berekend aan de hand van geometrische relaties. Hoe deze berekening precies tot stand komt, hangt af van de gebruikte meetmethode.

Een methode die veelal in GSM-netwerken wordt gebruikt, is Network Cell Identification (Cell-ID). De Cell-ID-methode gebruikt het middelpunt van het gebied dat een cell beslaat en de grootte van de cell om de positie van een mobiel apparaat binnen het cell-bereik te bepalen. De nauwkeurigheid van plaatsbepaling met Cell-ID hangt af van de vorm van de cell en de dichtheid van mobiele apparaten:

‘This density is used to determine the statistically most likely position of a user. It can also depend on the shape of a cell, which can vary considerably due to the geographic features of the cell, such as hills and large tall buildings.’

(Brimicombe en Li, 2009: 190)

Zo is bekend dat een mobiele telefoon in stedelijk gebied op 50 tot 500 meter nauwkeurig te positioneren is, maar dat in landelijk gebied de nauwkeurigheid varieert van 1 tot 35 kilometer vanwege grotere cellgebieden. Andere meetmethoden zijn Angle of Arrival (AOA), Time of Arrival (TOA), Time Difference of Arrival (TDOA) en Enhanced-Observed Time Difference (E-OTD) (Küpper, 2005).

Ahas en Mark (2005) laten zien dat het spatiotemporele gedrag van de samenleving kan worden onderzocht door mobiliteitsgegevens te koppelen aan de sociale identificatiegegevens waar mobiele telecomproviders over beschikken. Volgens de auteurs kunnen data over de chronologische spreiding van beweging in een stad bijvoorbeeld worden gebruikt in infrastructurele projecten. Ahas en Mark gaan in op het voorbeeld van ruimtelijke ordening in enkele steden in Estland (Ahas en Mark, 2005: 549). Daar werden kaarten gecreëerd die onder andere mobiliteitspatronen van verschillende leeftijdsgroepen gedurende één week visualiseerden.

5.2.4 Overige draadloze technologieën

Technologieën als Radio Frequency Identification (RFID), Wireless LAN (WiFi) en Bluetooth vallen in deze categorie. Deze groep technologieën heeft een vergelijkbare benadering als cell-gebaseerde communicatietechnologieën om de positie van een object te bepalen (Meints en Royer, 2007: 16). De locatie van een surveillanceobject wordt vastgesteld in de vorm van nabijheid tot één of meerdere basisstations.

RFID heeft twee basiscomponenten: de RFID-lezer en de RFID-tag, die onderling radiosignalen uitwisselen (Brimicombe en Li, 2009: 202; Küpper, 2005: 239-240). Er zijn passieve en actieve RFID-tags. Passieve tags hebben geen eigen energievoorziening en krijgen alleen energie via de radiosignalen die de RFID-lezer uitzendt. Passieve tags hebben doorgaans een kleine geheugencapaciteit met ruimte voor een beperkte hoeveelheid informatie, zoals een identificatienummer. Om te kunnen

communiceren met de RFID-lezer moet de passieve tag zich binnen een paar meter afstand bevinden. Dit is anders bij actieve RFID-tags die dankzij hun ingebouwde stroomvoorziening (bijvoorbeeld een batterij) in staat zijn op tientallen meters afstand signalen uit te wisselen met een lezer. Plaatsbepaling vindt plaats op het moment dat tag en lezer zich binnen de vereiste communicatieafstand bevinden:

‘When the user/device with a RFID tag moves into the communication range of a RFID reader, the reader prompts the tag and the antenna in the tag enables its chip to transmit the identification information to the reader. The reader then sends the information to the location server. In this way, the proximate position of a user/device can be obtained.’

(Brimicombe en Li, 2009: 202)

In dit geval is er sprake van een lezer op een vaste locatie en een mobiele tag, zoals bij de ov-chipkaart. RFID-plaatsbepaling kan echter ook plaatsvinden via vaste tags en mobiele lezers. Dan ontvangt de lezer de locatiegegevens van de tag, zodra hij daarbij in de buurt komt.

Wireless Local Area Networks (WLAN) zijn draadloze netwerken die vanaf het eind van de jaren 90 de vaste, bekabelde netwerken in kantoren en thuis zijn gaan vervangen. Een WLAN kan apparaten zoals computers, printers en mobiele telefoons met elkaar verbinden en toegang geven tot het internet. Wireless Fidelity (WiFi) is de meest bekende universele draadloze netwerkstandaard die in WLANs wordt gebruikt. Via WiFi kan een draadloos communicatienetwerk als extensie van een vast netwerk, zoals het internet, tot stand komen. Hiervoor zijn één of meerdere routers essentieel. Een router fungeert als toegangspunt (Access Point, AP) tot een draadloos of vast netwerk: ‘An AP has a radio transmitter, a receiver and an interface to other networks’ (Brimicombe en Li, 2009: 49). Een voor WiFi geschikt mobiel apparaat, zoals de meeste PDA’s, laptops en mobiele telefoons, krijgen via een router toegang tot een WLAN. Plaatsbepaling via WiFi vindt plaats door het meten van de ontvangen signaalsterkte bij twee of meerdere routers. WiFi-signalen met informatie daarin kunnen zowel door een mobiel apparaat als door een router worden verstuurd, waardoor de plaatsbepaling zowel in het netwerk als in het mobiele apparaat kan plaatsvinden. WiFi-plaatsbepaling werkt alleen in omgevingen met netwerkdekking via routers. De nauwkeurigheid is niet zo hoog en hangt af van de dichtheid van routers en de sterkte van het WiFi-signaal. Met deze plaatsbepalingstechnologie kan geen ruimtelijke locatie worden vastgesteld, maar wel een beschrijvende, bijvoorbeeld de vliegveldterminal waar een apparaat zich bevindt.

Bluetooth-technologie biedt ‘an ad hoc approach for a low power, short range wireless connection for voice and data transmission between various devices within a nominal

10 metre range’ (Brimicombe en Li, 2009: 49). In 1994 heeft Ericsson Mobile Communications Bluetooth in het leven geroepen om de haalbaarheid te onderzoeken van een goedkope en energiezuinige manier om een draadloze verbinding tussen verschillende vaste en mobiele apparaten te realiseren (Muller, 2003 in Brimicombe en Li, 2009: 49). De technologie is vernoemd naar Koning Harald Blåtand II, die in de tiende eeuw Denemarken en Noorwegen verenigde. Apparaten zoals mobiele telefoons, laptops en desktop computers kunnen via Bluetooth met elkaar communiceren indien ze ‘Bluetooth-enabled’ zijn en zich binnen 10 meter van elkaar bevinden. Op een mobiele telefoon kan bijvoorbeeld een Bluetooth transmitterchip zijn geplaatst. Dankzij de open standaard van de Bluetooth-radiofrequentie kan deze overal ter wereld worden gebruikt. Een ander voordeel is dat Bluetooth werkt zonder ingewikkelde installaties of een bepaalde set-up op de betrokken apparaten. Zodra Bluetooth-apparaten zich in elkaars buurt bevinden, start een zogenaamde service-discoveryprocedure. De apparaten wisselen dan berichten uit om elkaars aanwezigheid en mogelijke informatiediensten vast te stellen. Hoewel Bluetooth niet is ontworpen voor plaatsbepaling, maakt zijn inherente eigenschappen deze wel mogelijk. Een mobiel Bluetooth-apparaat is in staat om signalen met daarin een identificatiecode of profiel te verzenden en daarmee zijn nabijheid aan een Bluetooth-apparaat op een vaste locatie kenbaar te maken. Een andere, nauwkeurige plaatsbepalingsmethode met Bluetooth werkt op basis van signaalsterkte:

‘The received signal strength decreases logarithmically with distance both in indoor and outdoor environments. [...] The approximate position of a device will be the intersection of three circles generated by known signal levels from three different antennas.’

(Brimicombe en Li, 2009: 201)

5.2.5 *Sensorsystemen*

In tegenstelling tot de overige besproken plaatsbepalingstechnologieën maken sensorsystemen geen gebruik van radiosignalen. Biometrische systemen, infrarood-systemen en optische sensors zijn voorbeelden van sensorsystemen. Sensorsystemen werken tot op maximaal enkele meters afstand van het surveillanceobject (Meints en Royer, 2007: 17).

Camera’s met gezichtsherkenning, irisscanners en vingerafdruklezers zijn voorbeelden van biometrische systemen. Deze systemen worden gebruikt voor identificatie of verificatie van een persoon (Gasson, Meints en Warwick, 2005). Ze gelden als plaatsbepalingstechnologie op het moment dat de locatie van de gebruikte sensor bekend is.

Een infraroodsensor lokaliseert een apparaat of persoon op basis van nabijheid en wordt met name binnenshuis gebruikt (Brimicombe en Li, 2009: 203). Hiervoor is direct zicht tussen een zender en ontvanger vereist. Infraroodsignalen kunnen locatie-, tijds- en objectgegevens bevatten en ondersteunen tweezijdige communicatie. Doorgaans bevinden infraroodontvangers zich op vaste locaties en pikken ze signalen op van een zender op een apparaat of persoon (bv. polsbandje), zodra deze dichtbij genoeg is (1-2 meter).

Automatische nummerplaatherkenning (ANPR) is een voorbeeld van een systeem met optische sensoren. Een vaste of mobiele, met GPS uitgeruste camera neemt automatisch foto's van de kentekenplaten van alle passerende voertuigen. De onderliggende software vertaalt deze digitale foto's vervolgens in alfanumerieke data. De objectgegevens (fotobestanden en alfanumerieke data) worden opgeslagen samen met data over tijd en locatie.

Sensorsystemen worden bijvoorbeeld gebruikt voor verkeersmanagementdoeleinden:

‘A range of roadside and in-road devices using radar, acoustic sensors and infrared detectors are being increasingly deployed not only to count traffic and pedestrians round-the-clock but also to classify the traffic into vehicle types and to determine levels of congestion so as to provide near-instant warnings of events that are happening on our roads.’

(Brimicombe en Li, 2009: 151)

5.2.6 Chipkaartsystemen

Chipkaartsystemen, zoals betaal- of toegangspassen kunnen ook worden gebruikt voor plaatsbepaling. Bij een geldopname met een creditcard of bankpas wordt het unieke kenmerk van de betaalpas herkend door de pinautomaat en vervolgens samen met de overige actiegegevens opgenomen in een database van de kredietverstrekker of bank. De locatie van de pinautomaat en het tijdstip van de geldopname zijn onderdeel van de actiegegevens. Toegangspassen kunnen onthullen dat iemand (een deel van) een gebouw is ingegaan. De locatie van de kaartlezer is wederom bekend. Deze wordt op het moment van contact met de toegangspas gelinkt aan tijds- en objectgegevens.

Plaatsbepaling door een chipkaartsysteem kan alleen hoogst nauwkeurige momentopnames geven en geen continue mobiliteitsgegevensstroom, zoals wel mogelijk is in cell-gebaseerde communicatienetwerken en bij satellietssystemen.

5.2.7 *Hybride technologie*

In een hybride systeem worden meerdere typen plaatsbepalingstechnologieën gecombineerd om een hogere precisie en betere beschikbaarheid te bereiken. Een voorbeeld is Assisted GPS (A-GPS), waarbij GPS wordt gecombineerd met cell-gebaseerde technologie. Enkele nadelen van GPS, zoals de beperkte signaalontvangst binnenshuis en in druk bebouwde gebieden worden dan gecompenseerd door de cell-gebaseerde technologie die in beide gevallen wel goed werkt. Daar staat weer tegenover dat de beperkte nauwkeurigheid met cell-gebaseerde plaatsbepaling wordt aangevuld met de hoge precisie van GPS. Het basisprincipe van A-GPS is dat een mobiel netwerk dient om met aanvullende informatie en ondersteuning de locatie van mobiele apparaten met een GPS-ontvanger te bepalen. A-GPS kan op meerdere manieren werken. Zo kunnen methodes als Cell-ID en TDOA (zie 5.2.3) eerst grofweg de locatie van het mobiele apparaat vaststellen. Vervolgens kunnen de GPS-satellieten die op dat moment op die locatie zichtbaar zouden moeten zijn, worden geïdentificeerd, zodat het netwerk het mobiele apparaat kan instrueren om die specifieke satellieten te zoeken in plaats van ongericht op zoek te gaan naar satellieten die binnen bereik zijn. A-GPS kan ook de andere kant op werken. In dat geval worden GPS-ontvangers geïncorporeerd in het mobiele netwerk. Zogenaamde referentiestations ontvangen dan GPS-signalen en sturen deze via het netwerk naar het mobiele apparaat (Küpper, 2005: 226). Op het moment dat het apparaat zelf slechte GPS-ontvangst heeft, worden de locatiedata aangevuld met GPS-signalen via het netwerk.

5.3 Geografische informatiesystemen

Ruwe mobiliteitsgegevens zoals GPS-coördinaten of RFID-data hebben zonder context geen betekenis. Pas als we de coördinaten in een assenstelsel of, nog beter, op een kaart getoond krijgen, wordt duidelijk wat de data ons kunnen zeggen. Behalve deze voor interpretatie noodzakelijke omgevingsinformatie, is er nog een andere soort informatie die extra betekenissen kan genereren ten aanzien van de ruwe data. Het gaat dan om aanvullende informatie over het surveillanceobject zelf. Enerzijds gaat het om een soort identificatiecode van de mobiele apparatuur die het subject bij zich draagt, anderzijds gaat het om persoonsinformatie die mogelijk iets onthult over de identiteit van de gebruiker. Een geografisch informatiesysteem (GIS) is onontbeerlijk om de diverse stromen gegevens te managen en weer te geven. Het lokaliseren van personen in het kader van mobiliteitssurveillance kan gezien worden als onderdeel van een bredere trend tot geo-refereren. Bregt (2006: 6) spreekt zelfs van een ‘geo-informatie *community*’ die diverse informatie ‘geo-refereert’. Zaken die intrinsiek geen ruimtelijke dimensie hebben, dat wil zeggen, op natuurlijke wijze vastgeklonken zijn

aan het aardoppervlak, krijgen deze steeds vaker toebedeeld dankzij geo-informatietechnologie. Waar ruimtelijke informatie in de klassieke opvatting betrekking heeft op zaken als bestemmingsplannen, kadastrale kaarten, bodemgebruik of het weer, heeft deze tegenwoordig geheel nieuwe betekenissen gekregen. Persoonsinformatie die intrinsiek niet ruimtelijk van aard is, zoals inkomensgegevens, opleidingsniveau of samenstelling van het huishouden kan nu gekoppeld worden aan een plaats op de aarde en daarmee een ruimtelijke dimensie krijgen. Ongeveer 25 jaar geleden deden de eerste geo-informatietechnologieën hun intrede in publieke organisaties (Vonk, Geertman en Schot, 2007). Deze technologieën die het resultaat zijn van een verregaande samenwerking tussen onder andere cartografen, geografen en ICT'ers, vinden meer en meer hun weg binnen het openbaar bestuur. Zo lanceerde Politie Haaglanden in 2006 de website www.hoeveiligismijnwijk.nl, waarop burgers via een GIS-applicatie inzicht kunnen krijgen in de criminaliteit in hun buurt (De Kool en Van Wamelen, 2008: 297). Bregt (2006: 6) spreekt van 'de emancipatie van locatie' waarmee hij doelt op het sterk toenemende gebruik van locatiegebonden informatie in onze maatschappij.

Om weer te geven waar iets of iemand zich bevindt, wordt vaak een kaart gebruikt. De ouderwetse papieren kaart is echter niet toereikend om de complexe data die plaatsbepalingstechnologieën leveren te kunnen verwerken. Hier bieden geografische informatiesystemen uitkomst. Een GIS is meer dan een kaart. Het is een geautomatiseerd digitaal informatiesysteem betreffende locatiegerelateerde, op computers opgeslagen data (Black, 1997: 229). Een GIS kan er echter wel uitzien als een kaart op een computerscherm, maar dit is niet noodzakelijkerwijs het geval. De output van een GIS kan bijvoorbeeld ook de vorm hebben van een tabel of een lijst met gegevens. Enkele voordelen van een GIS worden duidelijk bij vergelijking met de traditionele papieren kaart (Vanneste, 2001: 86). Zo kunnen kaarten in een GIS digitaal verwerkt worden, waarbij schaal geen rol meer speelt en er geen limiet is aan de ruimte en het aantal objecten dat op de kaart kan worden weergegeven. De GIS-gebruiker kan bijvoorbeeld de keuze maken om de aanwezige personen in een bepaald gebied op de tijdstippen t en $t+1$ al dan niet tegelijk op een kaart af te beelden. Een ander voordeel is dat een grote database kan worden aangelegd met kenmerken van alle objecten op de kaart. Deze mogelijkheid bestaat voor zowel statische als dynamische objecten in een GIS. In het geval van personen kan het dan gaan om persoonsgegevens zoals nationaliteit of leeftijd van iemand die is uitgerust met een GPS-apparaat, die weergegeven wordt als een bewegend stipje op de kaart. Verschillende kaartlagen en attributen kunnen vervolgens op diverse manieren worden gecombineerd.

Samengevat is een kaart een statisch instrument, terwijl een GIS een dynamisch systeem is. Interessant in de context van het openbaar bestuur zijn de mogelijkheden van GIS voor analyse en toezicht door het combineren, visualiseren en correleren van

ruimtelijk verspreide data van personen en de daarbij horende kenmerken (Snellen, 2000). Vanneste (2001: 92) is echter terughoudend over het gebruik van GIS. Ze wijst erop dat GIS-gebruikers niet noodzakelijkerwijs professionele cartografen zijn en daarom lang niet altijd kaarten van goede kwaliteit produceren. Bovendien dreigt het gevaar dat gebruikers gedesillusioneerd raken wanneer ze volledig geautomatiseerde wonderen verwachten van GIS. GIS heeft dus veel potentieel dat niet altijd kan worden gerealiseerd vanwege de technische complexiteit. Een succesvolle inzet van GIS bij publieke mobiliteitssurveillance zal daarom deels afhangen van de kennis en vaardigheden van de beleidsmakers en burgers die hiermee in aanraking komen.

Onderstaand verhaal illustreert hoe een GIS-applicatie in een mobiele telefoon voor een eindgebruiker locatiegegevens vertaalt naar betekenisvolle en praktisch bruikbare mobiliteitsinformatie.

Op een zonnige dag loop ik het gebouw waar ik werk uit. Wegdromend bij het mooie weer heb ik plots geen idee meer waar ik nu ben. Ik haal mijn smartphone met ingebouwde GPS tevoorschijn en vraag informatie over mijn positie op. Op het scherm verschijnt een keurig lijstje met coördinaten, hoogte en nauwkeurigheid van de meting: breedte: N 51.5629°; lengte: O 5.0472°; nauwkeurigheid: 18 m; hoogte: 55 m; nauwkeurigheid: 35 m. Omdat ik geen kaart van het globale coördinatenstelsel afgebeeld op een wereldbol in mijn hoofd heb, heb ik behoefte aan aanvullende geo-informatie.

Basale geo-informatie

Daarom druk ik op de navigatietoets van mijn telefoon, waarop er een melding in beeld verschijnt dat mijn telefoon ijverig bezig is met de positiebepaling. Binnen een paar tellen wordt een kaartje getoond met een stip hierop. Die stip moet ik zijn, maar waar ben ik nu volgens de kaart? Deze toont enkele roze en groene vlakken en witte strepen en een balkje met '100 m' hierbij die ik achtereenvolgens als huizen, bomen, wegen en schaal van de kaart interpreteer.

Bestuurlijke informatie

Ook zie ik straatnamen verschijnen en ontdek na uitzoomen het predicaat 'Tilburg' bij het gebied waarin ik mij volgens mijn apparaat bevind.

Interessepunten

Na nog iets verder speuren op de kaart zie ik plots de aanduiding ‘Universiteit van Tilburg’ staan.

Met deze drie elementen heb ik de context om mijn locatiegegevens te interpreteren.

6 Conclusie

In informatietechnologische zin gaat het bij publieke mobiliteitssurveillance om het inwinnen, koppelen en analyseren/interpreteren van gegevens over mobiliteit. Mobiliteit bestaat uit twee aspecten: het surveillanceobject dat (mogelijk) beweegt en de beweging zelf. Mobiliteitsgegevens zijn dan ook gegevens over het surveillanceobject en gegevens van plaats en tijd. Het surveillanceobject kan een artefact, lichaam en/of actie zijn. Plaatsgegevens zijn onder te verdelen in ruimtelijke, netwerk-, en beschrijvende locaties. Gegevens van tijd kunnen het heden, het verleden of de toekomst beslaan. Het inwinnen van mobiliteitsgegevens kan gebeuren met behulp van een scala aan plaatsbepalingstechnologieën: satellietssystemen, netwerktechnologie, overige draadloze technologieën, sensorsystemen, chipkaartsystemen en hybride technologie. GIS-technologie dient om locatie-, tijds- en objectgegevens te managen, visualiseren en interpreteren tegen de achtergrond van geo-informatie. Verschillende actoren zijn met elkaar verbonden in de gegevensketen van inwinnen, koppelen en analyseren/interpreteren van mobiliteitsgegevens: het surveillanceobject, de content-leverancier, de informatieleverancier en de eindgebruiker. Kijkend naar de rollen die overheid en burgers kunnen vervullen, blijkt dat beiden soms meerdere informatierollen tegelijkertijd kunnen hebben.

Uit de in dit hoofdstuk verrichte literatuurstudie blijkt dat het eerste deel van de werkdefinitie van publieke mobiliteitssurveillance een aanpassing behoeft. De omschrijving *‘het op digitale wijze verzamelen en verwerken van mobiliteitsgegevens over al dan niet identificeerbare personen’* blijkt onnodig uitgebreid te zijn. De toevoeging *‘over al dan niet identificeerbare personen’* kan weggelaten worden, omdat mobiliteitsgegevens immers objectgegevens omvatten, waar gegevens over personen weer onder vallen.

In dit hoofdstuk heb ik voor publieke mobiliteitssurveillance laten zien wat voor gegevens de overheid over burgers kan verzamelen en verwerken en welke technologieën hierbij gebruikt kunnen worden. *Waarom* de overheid überhaupt geïnteresseerd is in mobiliteit van burgers, heb ik hiermee nog niet belicht. Dat deze

interesse vóór de opkomst van ICT allang bestond, maak ik duidelijk in het volgende hoofdstuk, waarin ik inga op de politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance.

HOOFDSTUK 3

DE POLITIEK-BESTUURLIJKE ACHTERGROND VAN PUBLIEKE MOBILITEITSSURVEILLANCE

1 Inleiding

Het vorige hoofdstuk heeft laten zien dat technologische ontwikkelingen van grote betekenis zijn voor hedendaagse praktijken van publieke mobiliteitssurveillance. Om te begrijpen wat publieke mobiliteitssurveillance is en wat dit fenomeen betekent voor de relatie overheid-burger is echter meer nodig dan een verhandeling over de informatie-technologische kenmerken. Het is immers niet alleen een ICT-toepassing, maar ook een overheidsactiviteit die is ontstaan vanuit bepaalde politiek-bestuurlijke behoeften en omstandigheden. In dit hoofdstuk besteed ik aandacht aan dit tweede aspect door de volgende deelvraag te beantwoorden: Wat is de politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance?

Om te begrijpen waarom de overheid geïnteresseerd is geraakt in informatie over de mobiliteit van burgers, besteed ik aandacht aan het historisch gegroeide belang van territoriale begrenzing. Geograaf Mark Monmonier en socioloog John Torpey leggen allebei een verband tussen het beheersen van mobiliteit van burgers en het definiëren en bewaken van territoriale grenzen. Monmonier (2010) legt dit verband in zijn betoog over wat hij gebiedende (imperative) en verbiedende (prohibitive) cartografie noemt:

‘Maps exert power in two ways: by shaping public opinion and by telling us where we can’t go and what we can’t (or must) do in specific places. [...] Whether blatant or subtle, the imperative map is usually intended either to stifle movement or to restrict an activity with a spatial dimension. Examples include aeronautical charts with “no-fly” zones, world political maps, and municipal zoning maps, backed up, respectively, by military aircraft, border guards, and code enforcement officers. [...] Whether the penalty for defiance is explicit or implied, an imperative map is a geographic threat that warns of unpleasant consequences. [...] Because efficient enforcement depends on well-defined territorial restrictions, the primary symbol on most prohibitive maps is the boundary line, underscored perhaps by labels and contrasting colors.’

(Monmonier, 2010: 1-2)

Voor Torpey (2000) is het wezen van de natiestaat de sleutel tot het begrijpen van de opkomst van het paspoort als beheersingsinstrument ten aanzien van de mobiliteit van burgers:

‘[...] the institutionalization of the idea of the “nation-state” as a prospectively homogeneous ethnocultural unit [...] necessarily entailed efforts to regulate people’s movements. Yet because nation-states are both territorial and membership organizations, they must erect and sustain boundaries between nationals and non-nationals both at their physical borders and among people within those borders. Boundaries between persons that are rooted in the legal category of nationality can only be maintained, it turns out, by documents indicating a person’s nationality, for there is simply no other way to know this fact about someone.’

(Torpey, 2000: 1)

Kaarten en het paspoort zijn blijkbaar van grote betekenis geweest bij de vaststelling van territoriale grenzen en de daarmee samenhangende beheersingsdrang ten aanzien van mobiliteit van burgers. Om de politiek-bestuurlijke historie van publieke mobiliteitssurveillance te verkennen, ga ik in dit hoofdstuk dan ook in op zowel cartografische ontwikkelingen als de opkomst van het paspoort. Allereerst werp ik een blik op de geschiedenis van de cartografie tegen de achtergrond van de opkomst van Europese staten en het bepalen van territoriale grenzen. Vervolgens besteed ik aandacht aan het paspoort als instrument om territoriale grenzen en de mobiliteit van burgers te beheersen. Daarna bespreek ik een belangrijke bedreiging van de territoriale basis van staten: de opkomst van ICT. Het daarmee gepaard gaande proces van deterritorialisering rafel ik uiteen in drie deelaspecten die ieder de territoriale basis van staten op een andere manier raken. Tenslotte trek ik een conclusie over de politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance.

2 Kaarten, staten en territoriale grenzen²²

2.1 De eerste kaarten: wereldvisie en ontdekkingstochten

Als we het over een kaart hebben, zullen de meeste mensen denken aan een gevouwen stuk papier met een schematische weergave van een bepaald geografisch gebied erop. In deze modernistische visie is een kaart een visuele reproductie van de werkelijkheid. Volgens Black (2004: 10) is het zinnvoller om een kaart te beschouwen als een weergave van ruimtelijke relaties. Deze weergave is niet noodzakelijkerwijs visueel en statisch, maar kan zich ook anders manifesteren, zoals in iemands verbale beschrijving van een route. Ruimtelijke relaties zijn dan meer dan geografische informatie over de hedendaagse wereld, maar kunnen ook betrekking hebben op situaties uit het verleden

²² Deze paragraaf is gebaseerd op het werk van Black (1997), tenzij anders aangegeven.

of in een andere werkelijkheid. In de middeleeuwen was het bijvoorbeeld gebruikelijk om religieuze en mythische symbolen te vinden op de *mappae mundi*, de kaarten van de wereld. Daarmee werd letterlijk een plaats (weer)gegeven voor religie in de wereld zoals men die toen kende. Uit de eerdere bespreking²³ van geografische informatiesystemen (GIS) en de trend tot geo-refereren is af te leiden dat er tegenwoordig meer ruimtelijke relaties worden gelegd dan in de begindagen van de cartografie.

Lang voor het ontstaan van nationale grenzen maakten mensen al kaarten. In de cartografische literatuur verwijzen vele auteurs naar inscripties in Babylonische kleitabletten als ze het hebben over de allereerste kaart ter wereld (Aber, 2004; Black, 2004; Joustra, Ter Mors en Galema, 2005; Van de Poel, 2001). Onder deze auteurs bestaat echter geen overeenstemming over de tijdsperiode waarin de eerste kaart werd vervaardigd. De schattingen lopen ver uiteen: van 3800 tot 500 voor Christus. Aan het begin van de vierde eeuw voor Christus zorgde Alexander de Grote voor een belangrijke bijdrage aan het maken van kaarten. Hij stuurde geografen erop uit om kennis te verwerven en vast te leggen over verkende zeeroutes (Black, 2004: 23). Griekse astronomen en geografen hebben veel bijgedragen aan onze kennis over de wereld. Zij ontwikkelden ideeën over de bolvorm van de aarde en gebruikten wiskunde om afstanden te berekenen.

Ptolemaeus, die actief was in de tweede eeuw na Christus, werd één van de beroemdste en meest invloedrijke Griekse wetenschappers. Het merendeel van zijn, voornamelijk geschreven, werk is goed bewaard gebleven en vormde een belangrijk startpunt voor de latere cartografie vanaf de vijftiende eeuw. Wel bestaan er twijfels of hij daadwerkelijk zelf zijn kaarten heeft getekend (Crone, 1978: 3). Desalniettemin zijn de door hem ontwikkelde projecties en coördinatensysteem van onschatbare waarde gebleken. Ook de Romeinen leverden een belangrijke bijdrage aan de cartografie, met name door het ontwikkelen van tekenen op schaal. De belangrijkste motivatie voor de Romeinen om kaarten te maken, was de groeiende behoefte om de wereld te veroveren en te domineren. Enerzijds maakten Romeinse generaals gebruik van kaarten om hun veldtochten te plannen. De Peutinger kaart (Tabula Peutingeriana) wordt beschouwd als de eerste routekaart ter wereld. Anderzijds dienden kaarten om macht tentoon te spreiden. Zo werd de grootschalige kaart *Forma Urbis Romae* tussen 203 en 211 na Christus in een muur van de Templum Pacis in Rome gegraveerd, zodat iedereen hem kon zien (Black, 2004: 24; Najbjerg, 2012).

²³ Zie hoofdstuk 2, paragraaf 5.3.

Er is weinig bekend over de Europese cartografie in de eeuwen direct na de val van het West-Romeinse rijk (476 na Christus). Crone (1978: 5) geeft aan dat ‘from the fifth to the tenth century, geographical knowledge was at a standstill in the western world’. Er bestaat slechts sporadische kennis over het praktische gebruik van kaarten in de Middeleeuwen. Wel zijn kaarten van andere, meer religieuze aard bewaard gebleven. Kijkend naar de *mappae mundi* wordt duidelijk dat de Bijbel in die tijd van grote invloed was op de perceptie van de wereld. Typisch op deze kaarten is de zogenaamde T-O-vorm: de continenten Azië, Europa en Afrika staan afgebeeld binnen een cirkelvorm (O), terwijl deze gescheiden worden door de T-vormige wateren in het midden van de kaart. De T-vorm symboliseert hierbij het heilige kruis. Daarnaast werden verschillende religieuze symbolen toegevoegd aan de kaart. Deze T-O-kaarten moeten vooral als een weergave van de toenmalig heersende perceptie van de wereld worden opgevat en niet zozeer als een machtsinstrument vanuit religieuze hoek. Een voorbeeld is de Hereford Mappa Mundi uit ongeveer 1300. Hierop is Jeruzalem het centrum van de wereld. Het oosten staat bovenaan getekend en toont onder andere het Hof van Eden in een cirkel aan de rand van de wereld. Groot-Brittannië is onderaan in het noordwesten afgebeeld. Er zijn weinig aanwijzingen dat kaarten in die tijd voor politieke doeleinden werden ingezet. Black (2004: 31) beweert dat tot midden veertiende eeuw de meeste kaarten in de wetenschap werden gebruikt. Vanaf die periode werden kaarten langzaamaan vaker voor praktische doeleinden gebruikt, maar waren verbale beschrijvingen nog altijd gebruikelijker.

2.2 Cartografie in de 15^e en 16^e eeuw: beginnend oog voor politiek en grenzen

De belangrijkste technologische ontwikkelingen in het premoderne tijdperk waren de ontwikkeling van de drukpers, triangulatie en schalen. De mogelijkheden voor verspreiding van kaarten veranderden radicaal met de uitvinding van de drukpers. In de jaren 1470 kwamen de eerste gedrukte kaarten uit in Europa en in de loop van de zestiende eeuw kregen gedrukte kaarten de overhand over handgetekende kaarten. Cartografen profiteerden van deze ontwikkeling, omdat deze de toegang tot recent gemaakte kaarten vergrootte, die ze konden kopiëren en aanpassen. Een nieuw, meer wijdverspreid publiek kon worden bediend, wat een impuls gaf aan de commerciële dimensie van cartografie. De uitvinding van triangulatie in 1533 zorgde ervoor dat cartografie objectiever en minder impressionistisch werd, doordat afstanden tussen twee punten op het ronde aardoppervlak nu gemeten konden worden door zijdes en hoeken van driehoeken te berekenen. Rond dezelfde tijd werd het gebruik van schaal, die oorspronkelijk door de Romeinen was uitgevonden, steeds gebruikelijker. Ondanks de verbeterde techniek, trokken kaarten nog altijd geen substantiële aandacht van de heersers van die tijd. Dit heeft mogelijk te maken met een nadruk op routes en

illustraties in de kaarten van die tijd, in tegenstelling tot de grenzen en territoria die te zien zijn op kaarten vanaf de zeventiende eeuw. Daarnaast domineerden de religieoorlogen West-Europa in de laatste helft van de zestiende eeuw, wat zorgde voor een verminderde koninklijke autoriteit (Clark, 1995: 36). Mercator, één van de belangrijkste geographen van de zestiende eeuw, vestigt in zijn *Atlas* uit 1595 al wel de aandacht op een nieuwe toegevoegde waarde van geografie: ‘it will contribute greatly to the knowledge of political regimes, providing that it describe²⁴ not only the position of various places, but also their nature or legitimate condition, which the duty of the geographer always demands’ (Crane, 2002: 250). Mercator voorzag dus al dat kaarten belangrijk zouden worden om geopolitieke verhoudingen weer te geven.

Black (2004: 31) geeft aan dat in de loop van de vijftiende eeuw langzaam een verandering optrad in de perceptie van grenzen. Men ontdekte dat kaarten de mogelijkheid boden om aan grenzen te denken in termen van lijnen in plaats van zones. Hierbij is het onderscheid tussen echte (real) en abstracte ruimtelijke informatie van belang (Government of South Australia, 2006; Wood, 1993: 7). ‘Echt’ betekent dan: wat we met onze zintuigen kunnen waarnemen. Het gaat dan bijvoorbeeld om bergen en rivieren die we kunnen zien op de wereld. Abstracte ruimtelijke informatie betreft een serie algemene, meestal van staatswege opgelegde afspraken, die de wereld wel vormgeven, maar niet zintuiglijk waargenomen kunnen worden. Jurisdicties, kavels en staatsterritoria zijn hier voorbeelden van.

Uit de zestiende eeuw zijn enkele voorbeelden van staatsgebruik van kaarten bekend. Ze werden onder andere gebruikt voor defensiedoeleinden, het vastleggen van routes en in diplomatieke onderhandelingen. Al rond 1540 toonden sommige kaarten locaties waar defensiewerken gebouwd konden worden en werden andere kaarten gebruikt voor het plannen, uitvoeren en uitleggen van routes (Black, 2004: 46). Ook is bekend dat kaarten werden gebruikt tijdens de onderhandelingen over het Engels-Franse verdrag van Ardres in 1546 (Black, 2004: 46). Het in kaart brengen van landgoederen gebeurde ook al in het zestiende-eeuwse Engeland. In die tijd waren al deze cartografische activiteiten echter geen onderdeel van de staatscultuur, wat ze in de achttiende eeuw wel zouden worden.

Monmonier (1996: 88-89) observeert dat deze eerste statelijke cartografische verkenningen aan het eind van de zestiende en begin van de zeventiende eeuw, naast een praktische functie, voor een belangrijk deel een symboolfunctie vervulden. Zowel de eenheid van het Engelse koninkrijk onder Elisabeth I als van het Franse koninkrijk

²⁴ De tekst die Crane hier citeert is vermoedelijk een oude Engelse vertaling van de originele Latijnse tekst, wat mogelijk verklaart waarom de *s* achter *describe* ontbreekt.

onder Henri IV werden benadrukt in de nationale atlassen die beide vorsten lieten maken. In treffende spottende stijl maakt Monmonier duidelijk hoe groot de symbolische kracht van kaarten is:

‘The map is the perfect symbol of the state. If your grand duchy or tribal area seems tired, run-down, and frayed at the edges, simply take a sheet of paper, plot some cities, roads, and physical features, draw a heavy, distinct boundary around as much territory as you dare claim, color it in, add name – perhaps reinforced with the impressive prefix “Republic of” – and presto: you are now the leader of a sovereign, autonomous country. Should anyone doubt it, merely point to the map. Not only is your new state on paper, it’s on a map, so it must be real.’

(Monmonier, 1996: 88)

Kaarten lijken dus een soort natuurlijke autoriteit te hebben, waar heersers en staten in latere eeuwen nog gretig gebruik van zouden maken.

2.3 Cartografie in de 17^e en 18^e eeuw: groeiende staatscontrole en staatsbelangen

Het cartografische inzicht om (staats)grenzen als lijnen weer te geven bestond weliswaar al in de loop van de vijftiende eeuw, maar de meeste heersers in Europa toonden pas aan het begin van de zeventiende eeuw belangstelling voor het verkrijgen van accurate kaarten van hun territoria. Zo stelde Henri IV van Frankrijk in 1607 koninklijke landmeters aan om alle grenzen en kustlijnen in kaart te brengen. Zijn beweegredenen voor deze opdracht kunnen teruggevoerd worden op de centralisatie van de Franse politieke macht die zich intussen had voltrokken. Deze machtscentralisatie was het resultaat van drie processen (Clark, 1995: 34). Ten eerste had de Franse monarchie haar machtsgebied uitgebreid. Ten tweede was de koninklijke macht gegroeid ten koste van die van de kerk en lokale adel. Een derde ontwikkeling was de afgenomen geografische mobiliteit van de Franse koningen. Het was onmogelijk geworden om persoonlijk alle plaatsen binnen het uitgebreide territorium te bezoeken. Omdat *La France* werd geregeerd vanuit een centrale residentie, Parijs of Versailles, is het aannemelijk dat de koning nieuwe manieren moest vinden om zijn territorium in de gaten te houden. De cartografie bood hiertoe mogelijkheden.

In de loop van de zeventiende en achttiende eeuw maakte de cartografie een enorme ontwikkeling door. Meer en meer van de nieuwe wereld en Europese kolonies werden in kaart gebracht. Hierbij ging het zowel om zeeroutes als de ontdekking van nieuwe kustlijnen. Nederlanders profiteerden van de toegenomen belangstelling voor de nieuwe wereld en zetten een aardige cartografische handel op. Door middel van kaarten konden directeuren van zeevaartmaatschappijen trots hun nieuwste ontdekkingen laten

zien. Tegelijkertijd bleef een steeds groter wordend publiek geïnformeerd over de overzeese handelsactiviteiten. Het is geen verrassing dat ook staatsleiders steeds meer oog kregen voor de voordelen die kaarten hun konden bieden. Militaire activiteiten ontwikkelden zich vervolgens steeds meer rond het gebruik van kaarten. In toenemende mate werden grootschalige militaire landverkenningen verricht. Legeringenieurs waren dan ook veelal verantwoordelijk voor de eerste gedetailleerde kaarten waarbij de nieuwste technieken werden gebruikt. Kaarten werden eveneens gemaakt om het publiek te informeren over militaire veldslagen. In 1666 stichtte de Franse koning Lodewijk XIV de *Académie royale des sciences* om toe te zien op militaire en economische activiteiten, de uitbreiding van wegen en kanalen, en de benutting van natuurlijke hulpbronnen. Hiermee zorgde hij tegelijkertijd voor een formele organisatie van de *ingénieurs géographes* die als landmeters werkten voor militaire en civiele eenheden (Crone, 1978: 85). Deze ontwikkeling laat zien dat de staat meer controle kreeg over cartografische activiteiten.

Behalve voor militaire doeleinden werden kaarten ook steeds meer gebruikt voor administratie en belastingen met betrekking tot landgoederen. De grenzen van landgoederen alsmede het eigenaarschap konden nu met grotere precisie worden bepaald. Deze toepassing van kaarten werd uitgebreid benut door de Zweden en later ook door de Fransen. Niet alleen werd met betrekking tot landgoederen het bewustzijn over grenzen vergroot, maar ook werden de grenzen van het staatsterritorium expliciet. Statelijke heersers gaven cartografen de opdracht om hun territoria vast te leggen, en met name de exacte locaties van de staatsgrenzen. Deze kaarten kregen een belangrijke rol in diplomatieke onderhandelingen en geschillen. Vanaf deze tijd werd het steeds gebruikelijker om een kaart op te nemen als onderdeel van een verdrag. In het Nederlands-Engelse verdrag van 1718 visualiseerde een kaart de grens tussen de Verenigde Provinciën en de Oostenrijkse Nederlanden (Black, 1997: 16). Cartografische activiteiten werden in de achttiende eeuw onderdeel van de staatscultuur, terwijl kaarten in de zestiende eeuw zoals gezien slechts sporadisch werden gebruikt voor staatsdoeleinden.

In de loop van de achttiende eeuw werden kaarten steeds nauwkeuriger en vervingen ze hun voorgangers vanwege een verbeterde methode voor lengtemeting die gecombineerd kon worden met triangulatie. Vanaf deze periode werden kaarten meer dan illustraties of decoraties, en veranderden in instrumenten ter weergave en actieve ondersteuning van de macht. De oprichting van topografische instituten in Frankrijk en Engeland laat eveneens zien dat staten kaarten belangrijk begonnen te vinden. Ten tijde van de Franse Revolutie en de Napoleontische tijd veranderden zowel de interne Franse grenzen als de grenzen binnen Europa. Deze nieuw opgelegde realiteit werd vormgegeven door kaarten te maken van de veranderde territoriale kenmerken. Deze ontwikkeling stimuleerde de vijanden van Frankrijk, zoals Engeland, om ook

cartografische projecten te starten. Staten verwierven controle over cartografische activiteiten door hier regulering voor in te stellen. Zo was het vanaf 1773 wettelijk verplicht om bij de constructie en het onderhoud van wegen kaarten te maken. The Ordnance Survey, het Britse Kadaster, werd in 1791 opgericht omdat:

‘The Government realised that in planning adequate defences to repel any invasion, the South Coast of England needed to be comprehensively and accurately mapped. So it instructed its Board of Ordnance – the defence ministry of its day – to speed the necessary survey work.’

(Ordnance Survey, 2007)

Cartografische activiteiten kwamen aan het eind van de achttiende eeuw meer en meer onder staatscontrole te staan en werden vaker in opdracht van de staat uitgevoerd.

2.4 Cartografie in de 19^e, 20^e en 21^e eeuw: staten maken kaarten en kaarten maken staten

Aan het begin van de negentiende eeuw was het ondenkbaar geworden om staatspolitiek te bedrijven zonder het gebruik van kaarten. Zowel kadastrale als topografische kaarten werden meer en meer geïnstitutionaliseerd van overheidswege. Ook werden kaarten nog nauwkeuriger dankzij een serie technologische doorbraken. De uitvinding van de stoommachine maakte massaproductie van papier en drukwerk mogelijk. Daarbij bood de lithografie nieuwe mogelijkheden voor het kopiëren, reviseren en reproduceren van kaarten. Verder werd de kleurenprint geïntroduceerd, waarmee kaartdetails op een andere manier zichtbaar konden worden gemaakt. Intussen nam de publieke belangstelling voor kaarten alleen maar toe, omdat men geïnformeerd wilde blijven over de oorlogen waar de natiestaten in waren verwickeld. Enerzijds vervulden de inmiddels bekende topografische kaarten deze informatie-functie door veldslagen en nieuwe grenzen af te beelden. Anderzijds werd rond 1870 een ander type kaart bekend, de satirische kaart. Deze bood de mogelijkheid om vanuit een kritische houding de spot te drijven met de (geo-)politieke stand van zaken. Satirische kaarten waren zowel in kranten, als op diverse afdrucken en ansichtkaarten te vinden (Joustra et al., 2005: 27). Deze ontwikkeling kan begrepen worden binnen de context van een groeiend nationalisme in Europa.

In de negentiende eeuw kwam nog een ander genre kaarten op: de thematische kaart. Deze veroverde al snel een stevige positie binnen de cartografie en genoot ook een groeiende publieke belangstelling. Dit type kaarten laat van een bepaald gebied niet alleen de basale geografische informatie zien, maar geeft ook informatie weer over de geografische verspreiding van andere typen verschijnselen, zoals ziektes,

populatiegegevens en geologische data. Thematische kaarten waren in eerste instantie met name voor de wetenschap van groot belang, maar blijken later ook navolging te krijgen in het openbaar bestuur als we kijken naar GIS-toepassingen. Zo is de weergave van mobiliteitsgegevens van burgers in een GIS te beschouwen als een hedendaagse thematische kaart.

Met het groeiende nationalisme in Europa werden kaarten steeds meer gebruikt om aan de hand van geschiedenis huidige politieke situaties uit te leggen en te legitimeren. Deze ontwikkeling illustreert dat kaarten macht uitoefenen door het vormgeven van de publieke opinie. In de historische atlas *Géographie historique de la France. Atlas spécial*, die onder Napoleon III werd gepubliceerd tussen 1854-1861, werd bijvoorbeeld bewijs geleverd van het heroïsche en succesvolle verleden van Frankrijk en werd kritiek geuit op de voorgaande regeringen (Black, 1997: 56). Dit gaf het volk een gevoel van trots over hun natie en verstevigde de positie van Napoleon III als hun heerser. Andere Europese naties produceerden ook historische atlassen ‘to play their part, in war as in peace, in confirming a sense of national destiny and continuity with a glorious past’ (Black, 1997: 101). Deze historische kaarten waren echter niet bedoeld om een zo volledig mogelijk beeld te schetsen van de geschiedenis. In tegendeel, geselecteerde historische gebeurtenissen kregen de nadruk om een bepaalde claim te maken en gebeurtenissen die dit doel niet ondersteunden werden weggelaten. In de (pre)Nazi cartografie zijn hiervan verschillende voorbeelden te vinden. Black (1997: 125) noemt het voorbeeld van een Duitse kaart die de grens van het keizerrijk in het jaar 1000 samen met de taalgrens verder naar het westen afbeeldt dan de werkelijke grens na de Eerste Wereldoorlog. Tijdens de Tweede Wereldoorlog waren de meeste kaarten echter van die tijd en lieten werkelijke en mogelijke herbepalingen van grenzen zien (Black, 1997; Monmonier, 1996). In de twintigste eeuw zorgden eerst luchtfotografie en later satelliettechnologie letterlijk voor een nieuw perspectief op cartografie. Deze nieuwe technologieën boden niet alleen een nieuw, meer up to date gezichtspunt van bovenaf, maar maakten dankzij geavanceerde meetmethoden ook zichtbaar wat men met het blote oog niet kon waarnemen. De nieuwe technologische mogelijkheden bleken van groot nut te zijn tijdens beide Wereldoorlogen en namen tegelijkertijd toe door de behoeftes tijdens de oorlog.

Aan het begin van de 21^e eeuw blijven militaire activiteiten van essentiële betekenis voor de cartografie en vice versa. Topografische instituten van de overheid blijven (inmiddels overwegend digitale) kaarten ontwikkelen voor militair gebruik, maar vinden nu ook andere klanten in de publieke en private sector. Tegelijkertijd zijn militaire cartografische verkenningen gunstig geweest voor de ontwikkeling van de cartografie, omdat ze nieuwe technische standaarden hebben gecreëerd en hebben bijgedragen aan de collectie staatskaarten. Een andere tak van cartografie, die van de kadastrale kaarten, heeft niet zo’n evident strategisch doel als de militaire cartografie,

maar is toch grotendeels in staatshanden. Door de controle over de kadastrale registratie heeft de overheid de juiste data in handen om eigendomsbelastingen te heffen. Daarnaast fungeert het kadaster als toetssteen bij eigendomclaims tussen burgers. De klassieke basis van staatsmacht, het monopolie op geweld en het heffen van belastingen, blijkt sterker dan ooit dankzij de hedendaagse cartografie.

Staten maken kaarten en kaarten maken staten. Kaarten geven politiek-geografische relaties weer en geven ze vorm. Het vastleggen van grenzen op een kaart is soms meer een creatie van de politieke werkelijkheid dan de weergave ervan. In die optiek zorgen kaarten ervoor dat er een paaltje in de grond gaat op de plek van de staatsgrens op de kaart, niet andersom. Zo gebruikten koloniale machthebbers kaarten om hun claims op Afrikaanse gebieden kracht bij te zetten: ‘That maps drawn up by diplomats and generals became a political reality lends an unintended irony to the aphorism that the pen is mightier than the sword’ (Monmonier, 1996: 90). Het lijkt er inderdaad op dat ‘maps work by serving interests’ (Wood, 1993) en dat het aantal en de diversiteit is toegenomen door de eeuwen heen. In de begindagen van de cartografie genoten kaarten slechts sporadische belangstelling van wetenschappers en reizigers. Sinds de achttiende eeuw heeft de cartografie een stevige positie op het politieke toneel verworven. Kaarten zijn in de loop der tijd uitgroeid tot zeer belangrijke informatiebronnen over de wereld en tegelijkertijd vormen ze een mechanisme om diezelfde wereld te ordenen. Grenzen op de kaart geven aan tot waar de legitieme macht van een staat reikt en tot waar bepaalde rechten en plichten gelden voor de mensen die het territorium betreden of zich al binnen het territorium bevinden. Dit is de imperatieve cartografie waar Monmonier het over heeft. In de volgende paragraaf ga ik nader in op het belang van staten om toegang tot en vertrek uit hun territoria te reguleren. Hierbij focus ik op de opkomst van het paspoort als essentieel instrument voor de regulering van mobiliteit. Tevens vormt het paspoort een verbindende schakel tussen het territorium en de gemeenschap van de natiestaat.

3 Regulering van mobiliteit: de opkomst van het paspoort²⁵

3.1 Introductie van het legitieme recht op beweging

Torpey (2000) maakt in zijn analyse van de opkomst en politiek-bestuurlijke betekenis van het paspoort duidelijk dat absolute heersers in het vroegmoderne Europa met name

²⁵ Tenzij anders aangegeven in de tekst, is deze paragraaf gebaseerd op het werk van Torpey (2000), waaruit een hoofdstuk opnieuw is gepubliceerd in de bundel van Hier en Greenberg (2007).

uit economische en militaire motieven belangstelling kregen voor de handel en wandel van burgers:

‘The mercantilist policies pursued by these states entailed the general presupposition that population was tantamount to, or at least convertible into, wealth and military strength. Accordingly, these rulers had a powerful interest in identifying and controlling the movements of their subjects.’

(Torpey, 2007: 61)

Zo maakten Duitse zeventiende-eeuwse heersers wetten om bedienden strakker aan hun meesters te verbinden en hen daarmee een onafhankelijke officiële status en de mogelijkheid om zelfstandig te reizen te ontzeggen. In Engeland werd in 1662 een wet van kracht die lokale autoriteiten de bevoegdheid gaf om eenieder uit hun gebied van jurisdictie te verwijderen die waarschijnlijk aanspraak zou maken op voorzieningen voor de armen, het zogenaamde ‘poor relief’. Aanvankelijk richtten heersers zich met name op het reguleren van de mobiliteit van mensen binnen hun rijken. De focus werd pas in de negentiende eeuw verlegd naar de externe grenzen, toen het kapitalisme en de natiestaat eenmaal hadden getriomfeerd.

Torpey (2007: 52) stelt dat ‘modern states, and the international state system of which they are part, have expropriated from individuals and private entities the legitimate “means of movement”, particularly, but by no means exclusively across international boundaries’. Hiermee zegt Torpey dat staten zich het recht hebben toegeëigend om de mobiliteit van hun eigen burgers en die van andere staten te reguleren. Identificatie-documenten, en met name het paspoort, zijn geïntroduceerd om de mobiliteit van (eigen en vreemde) burgers te meten (wie gaan het territorium in en uit) en te managen (wie mogen het territorium in en uit). Het moge duidelijk zijn dat het (cartografisch) vastleggen van territoriale grenzen een voorwaarde is om mobiliteit tussen verschillende territoria te kunnen beheersen. De relatie tussen het vastleggen van grenzen en het monitoren van bewegingen over deze grenzen gaat echter verder dan dat. Wederom laat ik Torpey (2007: 53) aan het woord: ‘[...] states’ monopolization of the right to authorize and regulate movement has been intrinsic to the very construction of states since the rise of absolutism in early modern Europe’. Zowel het bepalen van grenzen als het reguleren van mobiliteit zijn dus onlosmakelijk verbonden met het wezen van de staat.

3.2 Statelijke in- en exclusie: kwestie van gemeenschap en territorium

Het proces waarin staten legitieme mobiliteit monopoliseerden nam enkele honderden jaren in beslag en liep parallel aan de verschuiving van oriëntaties op het lokale naar

het nationale niveau. Deze verschuiving liep weer gelijk met de ontwikkeling van ‘nationale’ staten met eigen burgers vanuit de verscheidenheid aan rijken en kleine stadsstaten die zorgden voor een lappendeken op de kaarten van het vroegmoderne Europa. De groeiende statelijke regulering van mobiliteit ging hand in hand met een herdefiniëring van het wezen van de staat. Met het ontstaan van de natiestaat werd aan de notie van *waar* de staat is een notie toegevoegd van *wie* de staat is. Niet langer werd de staat zuiver gedefinieerd als territorium, maar ook als nationale gemeenschap.

De invoering van het paspoort ondersteunt de nieuwe verhouding tussen staat en burgers die gepaard ging met het ontstaan van de natiestaat. Torpey (2007: 57) spreekt van het omarmen (embracing) van de maatschappij door de staat: ‘...“surrounding” and “taking hold” of their members – individually and collectively – as those states grow larger and more administratively adept’. Het paspoort behorende bij een bepaalde staat is het formele lidmaatschapsbewijs van de gemeenschap van die staat, ofwel het bewijs van burgerschap. Torpey betoogt vervolgens dat de registratie – en daarmee erkenning – van burgers, die hoort bij de omarming, staten in staat stelt te overleven door inkomsten en opbrengsten uit de maatschappij zeker te stellen. Tegelijkertijd betekent het includeren van een groep mensen ook het uitsluiten van andere mensen om aanspraak te maken op voorzieningen van de staat. Enerzijds is het paspoort een uiting van burgerschap, anderzijds faciliteert het de opvatting van burgerschap als een status die iemand wel of niet kan hebben. Het paspoort is een uiting van burgerschap, die omschreven kan worden als: ‘*both* a set of practices (cultural, symbolic and economic) and a bundle of rights and duties (civil, political and social) that define an individual’s membership in a polity’ (Isin en Wood, 1999: 4). Het als tweede genoemde aspect van burgerschap als een status waarop een verzameling rechten en plichten van toepassing is, kan worden toegepast doordat het paspoort de registratie behelst van iemands identiteit. Binnen het ‘eigen’ staatsterritorium is het voor de meeste burgers duidelijk welke rechten en plichten hij heeft. Gaat hij echter met zijn paspoort in de hand naar een andere staat, dan is hij daar een stuk minder zeker van. Als toerist, tijdelijk arbeider, vluchteling of vreemdeling gelden voor hem andere rechten en plichten dan voor de staatsburgers aldaar. Zijn status is anders. Bij welke gemeenschap iemand hoort tezamen met in welk territorium hij zich bevindt, bepalen dus in hoge mate zijn status.

Iemand kan zijn status dan ook veranderen door naar een ander territorium te gaan en/of zich aan te sluiten bij een andere gemeenschap, waarbij het eerste doorgaans een voorwaarde is voor het tweede.²⁶ Hoe gemakkelijk of moeilijk een statusverandering

²⁶ Er zijn ook gevallen waarbij iemand een bepaalde nationaliteit toegewezen krijgt zonder ooit voet gezet te hebben in het bijbehorende territorium. Zo is iemand van rechtswege Nederlander indien één

kan plaatsvinden hangt af van de (inter)statelijke regulering van mobiliteit²⁷ van burgers. Hierbij gaat het om internationale verdragen over grensoverschrijdingen, zoals het Schengenverdrag en nationaal beleid op het gebied van immigratie en asiel. Dit is een dynamisch beleidsterrein dat zich mede onder de invloed van terroristische dreigingen in een razend tempo ontwikkelt en flink wordt bediscussieerd in juridische literatuur (Brouwer, Catz en Guild, 2003). Het paspoort is de spil in deze dynamiek, omdat dit zowel iets zegt over het al dan niet mogen overschrijden van landsgrenzen als over de politieke gemeenschap waar de houder toe behoort. Afhankelijk van zijn burgerschapsstatus en het territorium waar iemand zich bevindt, kan hij aanspraak maken op bepaalde rechten en onderworpen worden aan bepaalde plichten.

Met de invoering van het paspoort kregen staten een middel in handen om bepaalde mensen binnen de grenzen te houden, anderen juist buiten te zetten en weer anderen de toegang tot het territorium te ontfangen of juist te verwelkomen. Het functioneren van het paspoortstelsel hangt sterk samen met de territoriale basis van staat en maatschappij. Deze territoriale basis komt in recenter tijden onder druk te staan.

4 Staten onder druk: deterritorialisering

4.1 ICT versterkt en accelereert deterritorialisering

Territorialiteit vormt de kern van de staat. Staten oefenen macht uit binnen het door nationale grenzen bepaalde gebied en rechtsstaten zijn hierbij gebonden aan de voor hun eigen territorium geldende wet- en regelgeving en stellen deze op. De analyse van de historische ontwikkeling van de cartografie laat zien dat staten steeds meer belang zijn gaan hechten aan het (juridisch) vastleggen van territoriale grenzen ter legitimatie van hun machtsuitoefening. In de huidige netwerksamenleving zijn echter ontwikkelingen van deterritorialisering en virtualisering te zien waarin de legitimiteitsbasis van de natiestaat problematisch wordt als gevolg van globalisering en de hiermee verbonden mobiliteit en informatisering (Frissen, 1999; Kubben, 2007; WRR, 1998). De virtuele wereld wordt steeds belangrijker naast de fysieke wereld. Bijgevolg zijn mensen en processen minder vaak verbonden met een specifieke plaats of tijd. Daarnaast lijken de territoriale grenzen, die traditioneel staat en samenleving aan elkaar verbinden, te vervagen. Verschillende auteurs hebben dit proces van deterritorialisering

van zijn ouders Nederlander is. Hiervoor hoeft hij zelf niet naar Nederland te komen (Rijksoverheid, 2013a).

²⁷ In de zin van zowel ruimtelijke als sociale mobiliteit, zie hoofdstuk 2, paragraaf 2.1 voor een toelichting op dit onderscheid.

toegeschreven aan de verstrengeling van ICT – met name het internet – met dagelijkse activiteiten van burgers, bedrijven en publieke organisaties.

In 1998 publiceerde de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) het rapport ‘Staat zonder land’, waarin de raad deterritorialisering noemde als een belangrijke ICT-gerelateerde ontwikkeling. Wat is dan de betekenis van deterritorialisering? Letterlijk zou het ‘ongedaan maken van territorialisering’ of ‘verwijdering van territoriale kenmerken’ kunnen betekenen. In ieder geval verliest de notie van het territorium aan betekenis. The Oxford English Dictionary geeft ‘an area under the jurisdiction of a ruler or state’ als betekenis van ‘territory’ (Oxford University Press, 2008). Deterritorialisering zou dan kunnen duiden op een verminderd belang van het betreffende grondgebied of de macht van de bijbehorende institutie, of beide. Het proces van deterritorialisering kan zeker niet uitsluitend aan ICT-ontwikkelingen worden toegeschreven. ICT is echter wel als een zeer belangrijke oorzaak van deterritorialisering te beschouwen, die werkt als een versterker van andere oorzaken zoals internationalisering (Frissen, 1999; WRR, 1998) en de toegenomen mobiliteit van mensen (Pontier, 1997). ICT werkt in deze als versterker en accelerator vanwege haar eigenschappen van virtualisering en technologische turbulentie. Virtualisering maakt het mogelijk om gemakkelijk nieuwe, niet tastbare vormen van informatie te kopiëren en te verspreiden (Frissen, 1996). Technologische turbulentie heeft betrekking op de snelheid en onvoorspelbaarheid van technologische ontwikkelingen (Wetgeving voor de elektronische snelweg, 1998: 4).

De betekenis van deze deterritorialisering kan begrepen worden door drie categorieën van plaats te onderscheiden: macht over plaats, plaats als organiserend principe en eenheid van plaats. Ten eerste houdt deterritorialisering het verlies van macht over een bepaalde plaats in. De soevereiniteit van de staat creëert een monopolie op het gebruik van geweld, het heffen van belastingen en het maken van regulering binnen de nationale grenzen. Daarbij heeft de staat een autonome positie waardoor deze onafhankelijk van andere staten kan regeren. Deze territoriaal bepaalde macht wordt aangetast op het moment dat de schaal waarop beslissingen worden genomen, verandert. ICT heeft bijgedragen aan het destabiliseren van de traditionele, territoriaal gebonden, hiërarchische schalen, waarbij nieuwe sub- en supranationale schalen ontstaan die elkaar in toenemende mate lijken te overlappen (Frissen, 1999; Sassen, 2007). Een mogelijk gevolg is dat staten hun macht kunnen uitbreiden over grenzen heen, zoals de VS dat doen door het verzamelen en analyseren van passagiersgegevens. De hierdoor getroffen staten en burgers zien zich aangetast in het voorheen aan hen voorbehouden beschikkingsrecht over deze gegevens, waardoor er vanuit dit perspectief sprake is van verlies van macht. Dit betekent dat nationale grenzen en daarmee de notie van territorium er minder toe doen als het gaat om besturen in het internettijdperk. Ten tweede kan deterritorialisering begrepen worden als een

verminderd belang van plaats als organiserend principe (Snellen, 2000: 138). Online gemeenschappen worden gevormd vanuit gedeelde behoeften, interesses en doelen van mensen en niet zozeer vanwege fysieke nabijheid. De ‘death of distance’ die door het internet is veroorzaakt, verbindt bijvoorbeeld activisten van over de hele wereld (Capling en Nossal, 2001). Deze ontwikkeling kan worden gezien als een radicalisering van de toegenomen mobiliteit van mensen die reeds afstanden kleiner had gemaakt (Pontier, 1997). Functionele en temporele criteria zijn daarmee bepalender geworden voor de vorming van organisaties dan locatiegebonden criteria (Frissen, 1999). Staten worden gedwongen om over nationale grenzen heen te kijken wanneer ze met deze virtueel gevormde gemeenschappen omgaan. Een derde aspect van plaats, dat geraakt wordt door deterritorialisering is de eenheid van plaats. De WRR omschrijft deterritorialisering als een proces waarbij menselijke activiteiten of interactie tussen mensen niet langer eenduidig aan een specifieke en passende jurisdictie kunnen worden toegewezen (WRR, 1998). Actor, actie en gevolg kunnen dan niet meer verbonden worden aan één specifieke locatie. Dit aspect van deterritorialisering wordt veelal beschouwd als een typisch gevolg van het internet. Kenmerkend voor de virtuele wereld is de plaatsongebondenheid en de verminderde relevantie van tijd, dit in tegenstelling tot de fysieke wereld. Zo kunnen websites van overheidsinstanties tegelijkertijd bezocht worden door mensen uit verschillende continenten, waarbij geen kantoortijden of wachtrijen gelden. Virtuele ontwikkelingen spelen zich af voorbij het territorium. Vervolgens is het onduidelijk waar een bepaald proces eigenlijk plaatsvindt en welke nationale regels hierop van toepassing zijn.

4.2 Publieke mobiliteitssurveillance en deterritorialisering

Het verlies van macht over een bepaald gebied, de verminderde betekenis van plaats als organiserend principe en de afgenomen eenheid van plaats staan in contrast met het territoriaal georiënteerde openbaar bestuur. Frappant is dat de van ICT doordrenkte publieke mobiliteitssurveillance juist een focus op het vastleggen van plaats met zich meebrengt. ‘The state may be landing again’ stelt Snellen (2000: 138) over de opkomst van GIS in het openbaar bestuur. Wat zou publieke mobiliteitssurveillance kunnen betekenen voor de drie dimensies van plaats en daarmee voor de deterritorialisering van de staat?

Publieke mobiliteitssurveillance biedt de overheid mogelijkheden om macht over het territorium terug te winnen. Dit is bijvoorbeeld te zien in de inmiddels vervallen plannen voor het nieuwe Nederlandse beprijzingssysteem voor het weggebruik, waarbij de nieuwste satelliettechnologie gebruikt zou gaan worden. De overheid wordt in een dergelijk systeem in staat gesteld om functionele regelgeving, zoals wegenbelasting, te

relateren aan de feitelijke locatie van burgers. Hiermee kunnen alle gebruikers van het Nederlandse wegennet gevolgd worden en een rekening ontvangen. Het huidige wegenbelastingstelsel is beperkt tot de in Nederland geregistreerde voertuigeigenaren. Deze fictieve, administratieve weergave van de werkelijkheid zou door publieke mobiliteitssurveillance worden vervangen door de realiteit van GPS-signalen op de weg. Deze toegenomen kennis over mensen en plaatsen, ofwel ‘leesbaarheid van de samenleving’ betekent een grotere institutionele handelingsmacht (Scott, 1998). Bovendien neemt de macht over activiteiten binnen het territorium toe, omdat de overheid niet alleen dezelfde voertuigeigenaren beter kan monitoren en controleren, maar ook ongeregistreerde weggebruikers, zoals toeristen.

Daarnaast biedt publieke mobiliteitssurveillance mogelijkheden om plaats als organiserend principe weer belangrijk te maken. De betekenis van plaats lijkt echter op een radicale manier te veranderen. Tegenover de statische notie van plaats die wordt gevormd door het traditionele politieke territorium komt nu een dynamische vorm te staan. Activiteiten in het openbaar bestuur kunnen nu gedomineerd worden door een variatie aan veranderende plaatsen in plaats van een aantal traditioneel vastgestelde plaatsen. Een lokale overheid kan bijvoorbeeld een nieuwe wegeninfrastructuur implementeren gebaseerd op een analyse van mobiliteitsdata gegenereerd door mobiele telefoons (Ahas en Mark, 2005). De dynamische locatiegegevens, in tegenstelling tot het bij de institutie behorende territorium bepalen dan wat het gebied is waarvoor een verandering gewenst is. Deze nieuwe plaats kan evenwel onderdeel zijn van het territorium van de betreffende lokale overheid, maar kan de grenzen ook overschrijden waardoor meerdere politieke instituties gedwongen worden om samen te werken om het betreffende maatschappelijke probleem op te lossen. Functionele, temporele en locatiegebaseerde criteria bepalen dan hoe overheidsbeleid wordt gevormd. Deze dynamische plaatsen kunnen ook ontstaan doordat burgers bewust met elkaar communiceren op basis van fysieke nabijheid. Location-based mobile dating services zijn hier een voorbeeld van.²⁸ Abonnees van dergelijke diensten ontvangen een bericht op het moment dat een mogelijke ‘match’ in hun buurt wordt gedetecteerd. Dit voorbeeld laat zien dat publieke mobiliteitssurveillance de faciliteit biedt aan mensen om zich te organiseren gebaseerd op gemeenschappelijke interesses en locaties. Deze ontwikkeling leidt mogelijk tot nieuwe soorten publieke diensten, maar kan ook een uitdaging betekenen voor overheden als mensen met slechte bedoelingen zich op deze manier gaan organiseren. Ook al wint plaats als organiserend principe op deze manier weer aan betekenis, wil dat niet zeggen dat de gevolgen van deterritorialisering ongedaan worden gemaakt. Er is geen reden om aan te nemen dat de dynamische

²⁸ Voorbeelden zijn Meetmoi (www.meetmoi.com) en Streetspark (www.youtube.com/watch?v=PyT-KcW1abI)

plaatsen de gedeterritorialiseerde online gemeenschappen zullen vervangen. Het is op dit moment aannemelijker dat deze naast elkaar zullen bestaan.

Ook het verlies van eenheid van plaats in de fysieke wereld wordt niet tegengegaan door de inzet van mobiliteitssurveillance in het openbaar bestuur. Wel lijkt er sprake te zijn van een nieuwe eenheid van plaats in de virtuele wereld doordat mobiliteitssurveillance de virtuele en de fysieke wereld weet te verbinden. Informatie over waar een bepaalde persoon of groep van personen is of is geweest, kan nu gecombineerd worden met eerder niet gedeelde informatie van verschillende organisaties. De gecreëerde mobiliteitsinformatie kan aan de basis liggen van nieuwe methoden om afwijkend gedrag te detecteren of zelfs ongewenst gedrag te voorkomen. Tegelijkertijd ontstaat de mogelijkheid om publieke dienstverlening verder te personaliseren en op maat aan te bieden door geregistreeerde persoonlijke voorkeuren en andere individuele achtergrondinformatie te gebruiken om een burger op zijn mobieltje die informatie te verstrekken waar hij op een bepaalde locatie behoefte aan heeft. Het combineren en uitwisselen van mobiliteitsgegevens van burgers tussen verschillende overheidsinstanties is misschien niet direct bedreigend voor de privacy van burgers, maar de manier waarop deze gegevens gebruikt kunnen worden wel. Dit laatste is zeker het geval met de technische mogelijkheid om burgers ongevraagd op iedere straathoek een sms te sturen met een mededeling, vraag of misschien zelfs bevel, omdat ze op een bepaald moment op een bepaalde locatie zijn (De Hert, Nouwt, Voets et al., 2008).

Plaats en beweging worden op innovatieve wijze op de kaart gezet door publieke mobiliteitssurveillance. Dit betekent echter niet zonder meer dat de deterritorialisering van staat en samenleving wordt tegengegaan. Wel kan publieke mobiliteitssurveillance in het verlengde van de cartografische activiteiten van de overheid en de invoering van het paspoort begrepen worden als een poging om de macht over het eigen territorium te verstevigen. In het licht van de nog altijd doorzettende deterritorialisering is het de vraag of dit ook lukt.

5 Conclusie

Dit hoofdstuk heeft laten zien dat de hedendaagse publieke mobiliteitssurveillance meer is dan een nieuw ICT-speeltje in handen van de staat. Vanuit politiek-bestuurlijk oogpunt is de hedendaagse publieke mobiliteitssurveillance te begrijpen als een resultante van twee ontwikkelingen. Enerzijds is het een voortzetting van activiteiten die opkomende Europese natiestaten in de zeventiende en achttiende eeuw ontplooiden om hun territoriale grenzen vast te leggen en te bewaken: staatscartografie en de

ontwikkeling van het paspoort. Publieke mobiliteitssurveillance is zo gezien een moderne variant van het paspoort, met meer technologische mogelijkheden en toegepast op meerdere domeinen. Anderzijds is publieke mobiliteitssurveillance meer dan een voortzetting van reeds gebaande paden, maar is het een acceleratie hiervan die is ingegeven door twintigste-eeuwse bedreigingen van de territoriale basis van de staat: explosief toegenomen mobiliteit en de ICT-revolutie. Paradoxaal genoeg kan publieke mobiliteitssurveillance derhalve begrepen worden als een reactie op kenmerken van de ICT-revolutie waar ze tegelijkertijd zelf onderdeel van uitmaakt.

Zowel het bepalen van grenzen als het reguleren van mobiliteit, die beide aan de basis liggen van publieke mobiliteitssurveillance, zijn onlosmakelijk verbonden met het wezen van de staat. Staten oefenen macht uit binnen het door nationale grenzen bepaalde gebied en rechtsstaten zijn hierbij gebonden aan de voor hun eigen territorium geldende wet- en regelgeving en stellen deze op. De analyse van de historische ontwikkeling van de cartografie laat zien dat staten steeds meer belang zijn gaan hechten aan het (juridisch) vastleggen van territoriale grenzen ter legitimatie van hun machtsuitoefening. Macht en controle zijn zodoende centrale begrippen om de opkomst van publieke mobiliteitssurveillance te begrijpen. In het volgende hoofdstuk komen deze begrippen terug in de bespreking van surveillanceliteratuur. In de theorievorming over surveillance is in sterke mate een controleperspectief aanwezig. Ik stel echter vast dat het controleperspectief alleen onvoldoende handvatten biedt om de hedendaagse publieke mobiliteitssurveillance te begrijpen. Mobiliteitsinformatie wordt tegenwoordig niet zuiver ingewonnen om mobiliteit te reguleren. Het interactieperspectief en het voorzorgperspectief op surveillance onthullen in aanvulling op het controleperspectief andere logica's achter de surveillanceactiviteiten van de hedendaagse overheid.

HOOFDSTUK 4

SURVEILLANCE IN DE RELATIE OVERHEID-BURGER: CONTROLE, INTERACTIE EN VOORZORG²⁹

1 Inleiding

Om vanuit een bestuurskundige benadering de implicaties van publieke mobiliteitssurveillance voor de relatie overheid-burger te kunnen duiden, is inzicht nodig in het beleid dat daaraan ten grondslag ligt.³⁰ Bij de analyse van dit beleid richt ik mij op de onderliggende technologie- en legitimizeitsassumpties. Technologie-assumpties zijn veronderstellingen over de eigenschappen van surveillancetechnologie en de mogelijkheden die deze bieden in beleid. Legitimizeitsassumpties zijn veronderstellingen over de maatstaven aan de hand waarvan de aanwezigheid van surveillancetechnologie in beleid beoordeeld en al dan niet toegestaan moet worden. In surveillance- en e-governmentliteratuur zijn verschillende technologie- en legitimizeitsassumpties te vinden. In dit hoofdstuk groepeer ik deze in drie theoretische perspectieven op surveillance: het controleperspectief, het interactieperspectief en het voorzorgperspectief.³¹ De drie perspectieven verbind ik aan een typologie van drie verhoudingen tussen overheid en burger: machthebber-onderdaan, dienstverlener-cliënt en democratisch instituut-citoyen. Hierdoor wordt inzichtelijk welke theoretische verwachtingen ten aanzien van het gedrag van overheid en burgers voortvloeien uit ieder van de surveillanceperspectieven. De koppeling van surveillanceperspectieven aan overheids- en burgerverhoudingen resulteert in een theoretisch kader dat aan de basis ligt van de analyse van de casussen in het empirische deel van dit proefschrift. Dan zal duidelijk worden welke elementen van de drie surveillanceperspectieven te vinden zijn in de beleidspraktijken in de twee onderzochte casussen van publieke mobiliteitssurveillance in Nederland: ANPR bij de politie en de inwinning en verwerking van verkeersgegevens bij de Nationale Databank Wegverkeersgegevens (NDW).

²⁹ Delen van dit hoofdstuk zijn eerder gepubliceerd in Van Ooijen & Soeparman (2010) en Van Ooijen (2011).

³⁰ Zo licht ik reeds toe in hoofdstuk 1 van dit proefschrift.

³¹ In dit hoofdstuk behandel ik theorievorming die relevant is voor het begrijpen van de betekenis van surveillance voor de relatie overheid-burger. Inzichten over de gevolgen van surveillance binnen andere domeinen van de samenleving zoals de relatie tussen werkgever en werknemer en commerciële dienstverlening komen hier niet aan bod. Zie onder meer Lyon (2006a; 2007a) en Hier & Greenberg (2007) voor literatuur op deze terreinen van de *surveillance studies*.

Met de theoretische exercitie in dit hoofdstuk geef ik antwoord op de derde deelvraag: Welke perspectieven op surveillance in de relatie overheid-burger kunnen worden onderscheiden? Dit hoofdstuk is als volgt opgebouwd. Eerst werk ik in paragraaf 2 het begrip legitimiteit uit in drie dimensies: legaliteit, normatieve rechtvaardiging en maatschappelijke acceptatie. Hiermee ontstaan handvatten om de legitimiteits-assumpties binnen de drie surveillanceperspectieven te verduidelijken. In paragraaf 3 bespreek ik de drie typen verhoudingen in de relatie overheid-burger. In de drie volgende paragrafen behandel ik achtereenvolgens de hier onderscheiden controle-, interactie- en voorzorgperspectieven op surveillance. Voor ieder surveillanceperspectief volgt een theoretische en een narratieve verkenning. In de theoretische verkenning ga ik eerst op zoek naar de ideeën die ten grondslag liggen aan ieder perspectief: de onderliggende assumpties over de mogelijke beleidstoepassingen en legitimiteitsbeoordeling van surveillance. Vervolgens beredeneer ik welke invulling de relatie tussen overheid en burger theoretisch krijgt vanuit ieder surveillanceperspectief. Aansluitend illustreer ik ieder perspectief in een narratieve verkenning rondom de fictieve belevenissen van mevrouw Smit die onderweg te maken krijgt met verschillende surveillancetechnologieën, zoals ANPR, intelligente verkeerssystemen en burgertweets. Dit hoofdstuk besluit met een theoretisch kader waarin de opgedane inzichten over de implicaties van surveillance voor de relatie overheid-burger worden samengevat.

2 Legitimiteit als beoordelingscriterium van surveillance

2.1 Wat is legitimiteit?

Voordat ik in de paragrafen 4, 5 en 6 de technologie- en legitimiteitsassumpties van ieder surveillanceperspectief belicht, ga ik in deze paragraaf nader in op het begrip legitimiteit. Wat betekent legitimiteit en waarom is dit begrip relevant voor (surveillance in) het openbaar bestuur? Binnen de beleidswetenschappen is legitimiteit een bekend aangrijpingspunt bij het beoordelen van beleid (Abma en in 't Veld, 2001). Volgens Beetham zijn alle machtsstructuren op zoek naar legitimatie (Beetham, 1991). Legitimiteit is een maatstaf voor de kwaliteit van het openbaar bestuur en zodoende een belangrijk en leidend principe (Hendriks, 2007). Dit principe geeft de grenzen en verplichtingen aan voor het beleid en de daadwerkelijke acties van publieke organisaties, waardoor fundamentele rechten van burgers worden gewaarborgd. Het is tevens een complex principe vanwege de verschillende betekenissen en mogelijke interpretaties in de praktijk van het openbaar bestuur. Het onderwerp legitimiteit is vooral relevant in situaties waarin de publieke organisatie veel macht heeft in haar relatie met burgers (Zouridis, 2007). Een machtige organisatie kan nog machtiger

worden zodra zij informatie- en communicatietechnologie in het beleid en de beleidspraktijk heeft geïncorporeerd (Zuurmond, 1994). Met de inzet van surveillance wordt het onderwerp legitimiteit dus nog belangrijker. Vedder (2007a: 198) merkt op dat het streven naar legitimiteit zowel uit morele als uit praktische overwegingen kan plaatsvinden. In het tweede geval is legitimiteit instrumenteel om politiek effectief en efficiënt te handelen. Wat wordt in de literatuur dan verstaan onder legitimiteit?

Legitimiteit valt te omschrijven als ‘het gelijktijdig legaal en gezaghebbend zijn van een machtsconstellatie en de rechtvaardiging ervan’ (Zouridis, 2007: 97). Het verkrijgen, hebben en onderhouden van legitimiteit is verre van een gemakkelijke taak voor een publieke organisatie. Legitimiteit heeft te maken met de noodzaak tot het vervullen van criteria voor het recht op het uitoefenen van macht (Vedder, 2007c: 6). Het woord ‘recht’ dient hier niet alleen in juridische zin te worden opgevat, maar heeft een ruimere betekenis, zo blijkt uit literatuur over legitimiteit (Beetham, 1991; Vedder, 2007b; Zouridis, 2007; 2009). Met het Engelstalige ‘right to rule’, ofwel recht om te heersen, wordt eerder verwezen naar de grondslag of basis waarop een publieke organisatie haar machtsmiddelen mag inzetten. Dit recht om te heersen heeft meerdere dimensies en bestaat uit juridische, moreel normatieve en sociale aspecten (Vedder, 2007c: 7). Deze drie³² dimensies komen achtereenvolgens naar voren in Beethams conceptualisering van legitimiteit. Gezag is volgens hem legitiem wanneer:

- It is acquired and exercised according to established rules (legality).
- The rules are justifiable according to socially accepted beliefs about (i) the rightful source of authority, and (ii) the proper ends and standards of government (normative justifiability).
- Positions of authority are confirmed by the express consent or affirmation of appropriate subordinates, and by recognition from other legitimate authorities (legitimation).

(Beetham, 1991: 15-20)

Pas als aan deze aspecten is voldaan, dan is er sprake van ‘gezaghebbend machthebben’ (Hendriks, 2007) van de overheid jegens burgers. Achtereenvolgens

³² Meike Bokhorst doet in haar proefschrift (Bokhorst, 2014) een voorstel voor een conceptualisering van legitimiteit in vier dimensies, waar zij naast de juridische, ethische en sociale dimensies ook een politieke dimensie onderscheidt. Feitelijk rafelt zij het derde punt van Beetham, *legitimation*, uiteen in twee dimensies (politiek en sociaal), waar deze doorgaans als één dimensie (maatschappelijke acceptatie) wordt opgevat. Hoewel ik in een eerdere publicatie (Van Ooijen & Bokhorst, 2012) heb gewerkt met de vier dimensies van Bokhorst, ga ik in dit proefschrift uit van de meer conventionele driedimensionale conceptualisering van legitimiteit. Het gebruik van een vierde dimensie van legitimiteit vergt namelijk een fundamentele theoretische discussie van legitimiteit die niet plaatsvindt in dit proefschrift, maar in dat van collega Bokhorst.

bespreek ik de drie dimensies van legitimiteit: legaliteit, normatieve rechtvaardiging en maatschappelijke acceptatie.

2.2 Legaliteit, normatieve rechtvaardiging en maatschappelijke acceptatie

Legaliteit kan worden omschreven als het principe dat

‘de overheid burgers iets mag verbieden of gebieden [...], doch uitsluitend voor zover de wet dat uitdrukkelijk toestaat en op een manier die in overeenstemming is met de daarvoor geldende wettelijke regels en rechtsbeginselen.’

(Michiels, 2006: 11).

Er moet dus sprake zijn van recht en de waarden die het recht belichaamt. Dit aspect van legitimiteit verwijst naar conformiteit met regels. Dit lijkt wellicht een gemakkelijk te toetsen aspect van legitimiteit door simpelweg te bekijken of een bepaalde handeling in overeenstemming is met de geldende wet- en regelgeving. Er rijzen echter problemen op het moment dat blijkt dat er geen relevante regulering bestaat of slechts een algemeen geformuleerde regel die een hoge mate van interpretatie vereist om toepasbaar te maken op de specifieke beleidssituatie. Empirische indicatoren van legaliteit zijn verwijzingen naar wetten, regels en procedures.

Een tweede dimensie van legitimiteit is ‘de (inhoudelijke, materiële of morele) legitimatie van macht en machtsuitoefening’ (Zouridis, 2007: 114), ook wel aangeduid als rechtvaardiging of verantwoording. Dit aspect van legitimiteit gaat over rechtvaardiging in termen van inhoudelijke, materiële of morele normen en waarden. Ook al is dit het enige legitimiteitsaspect dat inhoudelijke criteria kan bevatten (normen en waarden met een specifieke inhoud), zoals respect voor mensenrechten, beperkt het zich niet tot dit type criteria. Procedurele normen zoals rekenschap en verantwoording kunnen hier ook bij horen (Vedder, 2007c: 8).

De derde legitimiteitsdimensie, maatschappelijke acceptatie, betreft de toestemming of vertegenwoordiging van diegenen die betrokken zijn bij of getroffen worden door het beleid. Voor maatschappelijke acceptatie bestaan drie indicatoren: steun, vertrouwen en gehoorzaamheid (Zouridis, 2009: 299). Daarbij is het van belang dat het niet alleen een kwestie is van acceptatie onder burgers, maar dat het ook om het raadplegen van machtige of ter zake kundige organisaties gaat (Vedder, 2007a: 204).

Het is de vraag of aan alle legitimiteitsdimensies moet worden voldaan om legitiem te zijn. Op basis van de eerder genoemde definitie van legitimiteit van Zouridis (2007) zou beleid inderdaad aan alle dimensies moeten voldoen. Uit Beethams benadering

blijkt echter dat enige mate van illegitimiteit onvermijdelijk is (1991, geciteerd in Sparks, Bottoms en Hay, 1996: 85). Beethams schema toont in iedere dimensie een vorm van niet-legitieme macht. De auteur maakt een onderscheid tussen illegitimiteit (overtreding van regels), een legitimiteitsstekort (discrepancie tussen regels en ondersteunende gedeelde overtuigingen of afwezigheid van gedeelde overtuigingen) en de-legitimatie (intrekking van toestemming). Alle drie de vormen van niet-legitieme macht zijn realistische opties die een organisatie zou moeten voorkomen. Hierbij is de normatieve dimensie logisch superieur aan zowel de juridische als de sociale dimensies van legitimiteit, omdat de laatste twee instrumenteel kunnen zijn voor het voldoen van de eerste (Vedder, 2007a: 210). Copp maakt een vergelijkbaar punt met zijn stelling dat morele autoriteit cruciaal is voor legitimiteit (1999: 3).

Wat de beoordeling van legitimiteit ook lastig maakt is dat legitimiteit niet in absolute termen gedefinieerd kan worden. Ideeën over wat legitiem is, veranderen door de tijd heen. Criteria zoals wetten en maatschappelijke opvattingen zijn aan verandering onderhevig, wat het lastig maakt om surveillancebeleid hierop af te stemmen. Beetham stelt dat de specifieke inhoud van legitimerende principes grotendeels historisch en cultureel variabel is (zie Sparks, Bottoms en Hay, 1996: 85). Wat in de jaren '70 het handelen van een overheidsorganisatie legitimeerde, kan vier decennia later wel eens als niet legitiem worden beschouwd. Deze variabiliteit in evaluatiecriteria compliceert de beoordeling van surveillance vanuit legitimiteitsoogpunt in hoge mate. Is het bijvoorbeeld legitiem als een publieke organisatie anticipeert op toekomstige gebeurtenissen om haar handelen te legitimeren?

Samen met technologieassumpties zijn de legitimiteitsassumpties in een bepaald surveillancebeleid een belangrijke factor in de vormgeving van de relatie tussen overheid en burger. Hoe juridische regels worden geïnterpreteerd, welke normen en waarden van belang worden geacht en in hoeverre publieke steun wordt verwacht, beïnvloeden de ontwikkeling van beleid en daarmee de manier waarop de overheid en burgers met elkaar te maken hebben. Om te kunnen analyseren wat bepaalde legitimiteits- en technologieassumpties naar verwachting betekenen voor de relatie overheid-burger is het eerst nodig de relatie overheid-burger theoretisch uit te werken.

3 De relatie overheid-burger

3.1 Inleiding

De relatie overheid-burger is uiterst ambigu, omdat een burger iemand is die in staat is te regeren, maar ook om geregeerd te worden (Van Gunsteren, 1992). Zo geeft de

overheid door middel van beleid richting aan het handelen van burgers, maar kunnen burgers door te stemmen en via interactieve beleidsvorming juist zelf invloed uitoefenen op beleid. Tegelijkertijd wil de overheid in haar dienstverlening tegemoet komen aan de wensen van burgers, maar heeft ze ook de macht om de afname van bepaalde diensten af te dwingen. Kortom, overheid en burgers hebben in verschillende hoedanigheden met elkaar te maken, die op gespannen voet staan met elkaar.

Uit bestaande conceptualiseringen van de relatie overheid-burger kan worden afgeleid dat overheid en burger in hoofdlijnen drie verhoudingen kunnen hebben ten opzichte van elkaar (Boogers en Thaens, 2004; Mintzberg, 1996; Tops en Zouridis, 2000). Ten eerste heeft de overheid in de rol van machthebber de burger als onderdaan tegenover zich. Ten tweede ontmoet de overheid als dienstverlener de burger als cliënt. Ten derde heeft de overheid als democratisch instituut een relatie met de burger als citizen. Deze rollen representeren de verschillende petten die overheid en burgers (soms tegelijkertijd) op hebben en waarin ze elkaar kunnen benaderen. Boogers en Thaens (2004: 18) merken terecht op dat het voor zich spreekt dat ‘de “schotten” tussen deze rollen in de praktijk niet geheel waterdicht zijn’. De theoretische onderverdeling dient net als bij Mintzberg (1996: 78) ‘not so much for classification as for clarification – to further our appreciation of the varied purposes of government’. Wat zijn dan de kenmerken van deze drie verhoudingen binnen de relatie overheid-burger?

3.2 De verhouding machthebber-onderdaan

In de rol van onderdaan draait het voor de burger om de plichten die hij volgens de overheid heeft, zoals het betalen van belastingen en zich fatsoenlijk gedragen in het verkeer. Wanneer de overheid de burger benadert als onderdaan heeft zij zelf de rol van machthebber die wet- en regelgeving en gedragsrichtlijnen kan opstellen en handhaven om het gedrag van burgers te sturen. De overheid doet in deze verhouding beroep op haar autoriteit, legitimiteit of gezag om bepaald gedrag te stimuleren of juist te ontmoedigen (Tops en Zouridis, 2000). Ook al doet deze omschrijving wellicht denken aan tirannieke staten uit vroegere tijden, dit machtsaspect is nog altijd duidelijk aanwezig bij de moderne overheid: ‘in one way or another we all remain subjects of our governments – when we pay taxes, allow ourselves to be drafted into armies, or respect government regulations for the sake of collective order’ (Mintzberg, 1996: 77). Naast wet- en regelgeving en financiële prikkels kan de overheid communicatie inzetten als beleidsinstrument om de onderdaan aan te spreken:

‘Door burgers te overtuigen van de juistheid en onjuistheid van maatschappelijk gedrag gaan burgers zich beter gedragen, zo luidt de veronderstelling achter deze campagnes. Denk hierbij bijvoorbeeld aan de spotjes die oproepen tot energiezuinig, duurzaam en sociaal correct gedrag.’

(Tops en Zouridis, 2000: 14)

Als onderdaan zit de burger duidelijk in een passieve rol aan de ontvangende kant van besluitvorming (Tops en Zouridis, 2000). Kortom, in de verhouding machthebber-onderdaan richt de overheid zich op het opstellen en handhaven van regels, en de burger op het kennen en naleven hiervan.

3.3 De verhouding dienstverlener-cliënt

‘To paraphrase John F. Kennedy, the question for us as subjects is what we must do for our governments in the form of respecting state controls. In contrast, as clients who receive professional services, our question is about what the state provides to us.’

(Mintzberg, 1996: 77)

Als cliënt zit de burger eveneens aan de ontvangende kant van besluitvorming, maar lijkt de nadruk in eerste instantie minder op de plichten en meer op de aanspraken die hij krijgt van de overheid. De dienstverlening die de overheid biedt aan haar burgers als cliënten staat centraal. Het garanderen van goede zorg en onderwijs zijn hier voorbeelden van. Ondanks de populariteit van het klantdenken in overheidsdienstverlening (Hoogwout, 2010) is het misleidend om burgers in dezen als klant te bestempelen:

‘I am not a mere customer of my government, thank you. I expect something more than arm’s-length trading and something less than the encouragement to consume.’

(Mintzberg 1996: 77)

De bedrijfsmatige term klant impliceert een vrijblijvendheid en keuzevrijheid in het spel van vraag en aanbod die de burger als cliënt niet geniet. Hoe vrijblijvend is het om de dienst af te nemen die de overheid heeft ontwikkeld om internationaal te reizen: het paspoort? Hoeveel keuze van aanbieders heeft een ouder die een kindgebonden budget wil aanvragen? In de benadering van haar cliënten richt de overheid zich met name op het begrijpelijk, toegankelijk of makkelijk maken van de beschikbare diensten (Tops en Zouridis, 2000). Overheidsdiensten hebben niet exclusief met rechten van burgers te maken, maar soms ook met plichten. In die gevallen is er in het geheel geen sprake van vrijblijvendheid bij het ‘genieten’ van dienstverlening en komen de burgerrollen van

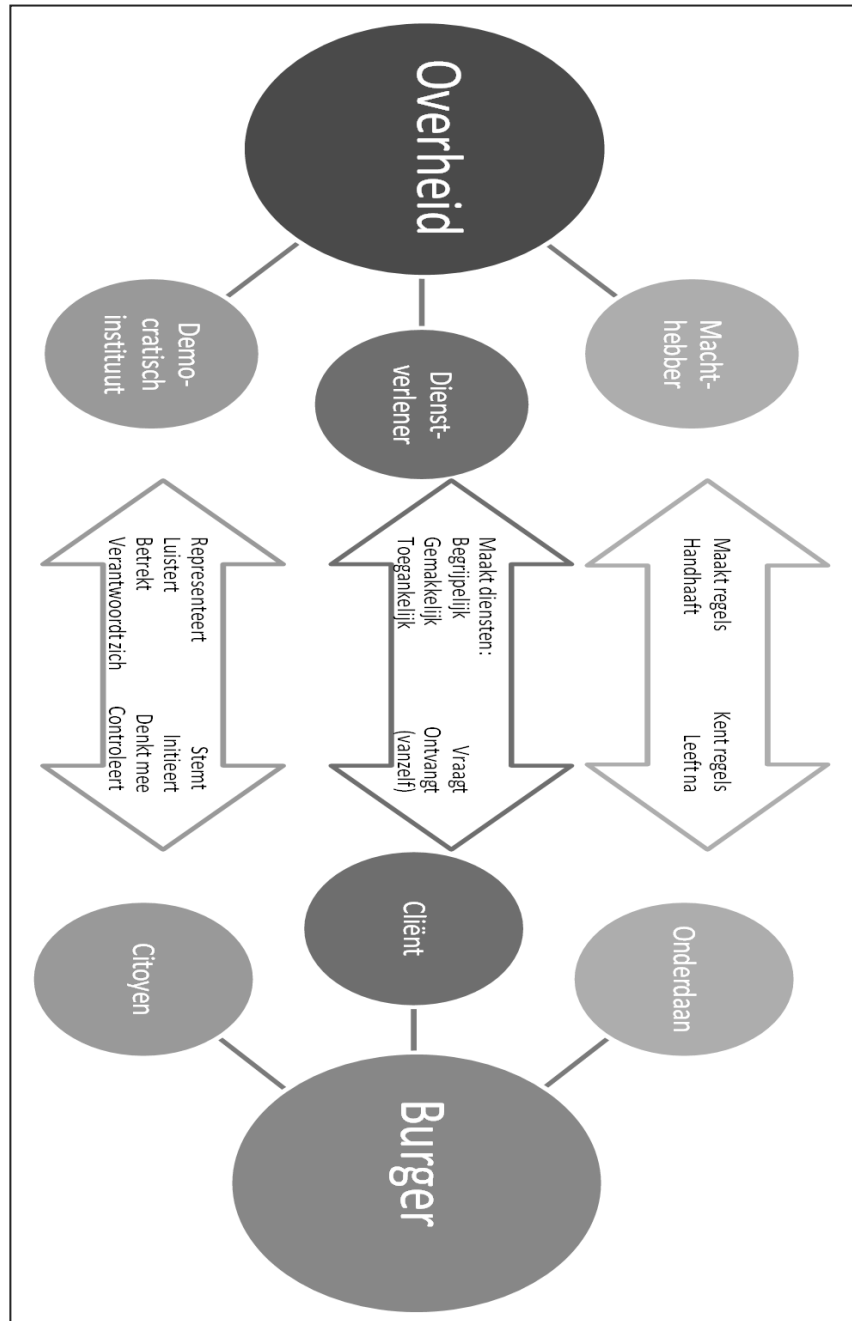
cliënt en onderdaan dicht bij elkaar. De belastingaangifte is een bekend voorbeeld van zo'n verplichte dienst. De overheid verplicht de burger als onderdaan om aangifte te doen en probeert dit proces zo makkelijk mogelijk te maken voor de burger als cliënt. Passend bij de vervlechting van burgerrollen promoot de Belastingdienst haar dienstverlening al jaren met de slogan 'Leuker kunnen we het niet maken, wel makkelijker'. Kortom, in de verhouding dienstverlener-cliënt richt de overheid zich op het begrijpelijk, gemakkelijk en toegankelijk maken van diensten, en de burger op het aanvragen en (vanzelf) ontvangen hiervan.

3.4 De verhouding democratisch instituut-citoyen

In tegenstelling tot de burgerrollen van onderdaan en cliënt draait die van citoyen om actief staatsburgerschap en bevindt zich daarmee meer aan de 'opdrachtgevende' kant van besluitvorming (Tops en Zouridis, 2000). Boogers en Thaens (2004: 20) noemen vier typen contacten tussen overheid en citoyen: representatie, het genereren van ideeën, besluitvorming en controle/verantwoording. Representatie draait om de vertegenwoordiging van de burger in het politieke systeem, bijvoorbeeld als lid van een politieke partij of als kiezer. Bij het genereren van ideeën zijn burgers actief als mogelijke initiators van beleid of worden ze behandeld als partners in een beleidsvormingsproces. Kortom, in deze verhouding doet de mening van de burger ertoe. Betrokkenheid van citoyens in besluitvorming kan bijvoorbeeld in referenda of inspraakprocedures plaatsvinden. Ten vierde zijn controle en verantwoording belangrijke aspecten in de relatie democratisch instituut-citoyen. Hierbij gaat het om inzage van burgers in de activiteiten van de overheid en het rekenschap dat diezelfde overheid van die activiteiten geeft. Mediaoptredens van bestuurders en rapporten van onderzoekscommissies zijn hier voorbeelden van. Waar bij de onderdaanrol de overheid het gedrag van burgers wil sturen, is het bij de citoyenrol precies omgekeerd. De democratische rechten van burgers en plichten van de overheid staan centraal. Voor de overheid is aandacht voor de relatie met de burger als citoyen belangrijk om maatschappelijk draagvlak voor beleid te realiseren (De Graaf, 2007; Tops en Zouridis, 2000). Kortom, in de relatie democratisch instituut-citoyen richt de overheid zich op het representeren van, luisteren naar, betrekken van en verantwoording afleggen aan burgers. De burger manifesteert zich als citoyen door te stemmen, beleid te initiëren, mee te denken en de overheid te controleren.

3.5 De relatie overheid-burger en surveillanceperspectieven

Figuur 4 geeft schematisch de drie verhoudingen binnen de relatie overheid-burger weer.



Figuur 4: De relatie overheid-burger

De verhoudingen van machthebber-onderdaan, dienstverlener-cliënt en democratisch instituut-citoyen benadrukken ieder een ander essentieel aspect van de relatie overheid-burger. Om de relatie tussen overheid en burgers onder bepaalde omstandigheden – in dit onderzoek het bestaan van publieke mobiliteitssurveillance – te beschrijven, moet aandacht besteed worden aan alle drie de verhoudingen. Hoe kunnen deze theoretisch worden ingevuld als er sprake is van surveillance? Hoe gaan deze drie verhoudingen er uitzien met de aanwezigheid van surveillancetechnologieën in het openbaar bestuur? Wat betekent surveillance bijvoorbeeld voor het maken en handhaven van regels (overheid als machthebber) en het kennen en naleven hiervan (burger als onderdaan)? In de volgende paragrafen wordt duidelijk dat het antwoord varieert afhankelijk van het gehanteerde theoretische perspectief op surveillance. Hierbij onderscheid ik drie theoretische surveillanc perspectieven: controle, interactie en voorzorg. Deze perspectieven laten ieder andere assumpties zien over de eigenschappen van surveillancetechnologie en welke mogelijkheden deze bieden in beleid (technologie-assumpties), en over de maatstaven aan de hand waarvan de aanwezigheid van surveillancetechnologie in beleid beoordeeld en al dan niet toegestaan moet worden (legitimiteitsassumpties), en daarmee logischerwijs ook over de implicaties voor de relatie overheid-burger.

4 Het controleperspectief

4.1 Big Brother is watching you

‘BIG BROTHER IS WATCHING YOU’ (Orwell, 1949: 2). Vanuit het controleperspectief moeten burgers in de surveillancestaat op hun tellen passen. Ze mogen zich niet afwijkend gedragen. Dat heeft de hogere macht in de gaten. Deze heeft immers af luisterapparatuur, camera’s en andere sensoren tot zijn beschikking om te detecteren of ze uit de toon vallen. In de hedendaagse informatiesamenleving is surveillance alomtegenwoordig. We kunnen zelfs spreken van een surveillance society (Lyon, 2007b) waarin surveillancetechnologie in alle facetten van onze levens is doorgedrongen.

De controlestaat die George Orwell (1949) schetst in zijn *1984* vormt een krachtig schrikbeeld: ‘Dit nooit’. Het relaas van een maatschappij waarin burgers zich, al dan niet bewust, conformeren aan de wil van de staat zien we terugkeren in verschillende hoedanigheden: van ‘surveillance state’ (Taylor et al., 2009) en ‘controlestaat’ (Vedder, Van der Wees, Koops et al., 2007) tot ‘panoptic state’ (Bannister, 2005). De aangehaalde, beroemde leuze van Big Brother krijgt de lezer van *1984* meteen in zijn greep en heeft door de jaren heen eerder aan kracht gewonnen dan verloren. Deze frase

is het adagium geworden van het controleperspectief. Net als in Orwells roman is deze zowel een afschrikwekkende waarschuwing als een weergave van hoe surveillance werkt. Foucaults filosofische bewerking van Benthams panopticon fungeert in het controleperspectief als de tweede krachtige metafoor voor surveillance (Haggerty en Ericson, 2007: 105). Haggerty (2006: 25) vat deze bewerking als volgt samen: ‘Panoptic schemes, following Foucault, become a principal means for managing a host of different populations through the dispersion of disciplinary power more generally’. Dit is echter een vrij eendimensionale interpretatie van Foucaults opvatting van macht. Hij benadrukte juist dat macht een relationeel begrip is, waarbij er geen sprake is van één partij die macht zou hebben of bezitten. In plaats daarvan bestaat macht pas zodra twee partijen daaraan meedoen: een partij die macht uitoefent en een partij die macht ondergaat en de normen van de andere partij internaliseert. Zowel Orwell als de panopticonmetafoor maakt duidelijk dat de kennis die staat en burgers al dan niet over elkaar hebben cruciaal is voor het functioneren van de controlestaat. Wat weet de staat (niet) van burgers en wat weten burgers (niet) van de staat?

4.2 Disciplineren in het elektronisch superpanopticon

In het controleperspectief binnen de surveillance studies wordt Jeremy Benthams stenen panopticon getransformeerd tot een elektronisch superpanopticon (Lyon, 2001b: 328). Poster (1990: 93) beschrijft dit als ‘a system of surveillance without walls, windows, towers or guards’. De fysieke wachttoren is in dit systeem veranderd in een datacentrum. Het centrale principe van kennisasymmetrie blijft in de elektronische versie bestaan en heeft twee elementen. Ten eerste is er nog altijd een tweedeling tussen degenen die kijken en degenen die bekeken worden. ‘Each individual [...] is seen, but he does not see; he is object of information, never a subject in communication’ (Foucault, 1979: 303). Bij surveillance als controle is het in eerste instantie de overheid die kijkt en de burgers die bekeken worden, en niet andersom. Zo kunnen opsporingsdiensten burgers traceren via hun mobiele telefoon en kan stadstoezicht het winkelend publiek via camerasurveillance in de gaten houden. Voor burgers is het echter moeilijker om de gangen van de overheid na te gaan. Zo hebben burgers geen toegang tot actuele GPS-data om te controleren of politie en ambulance op tijd zijn uitgerukt na melding van een ongeval. De overheid weet door haar rol als kijker veel meer over het gedrag van burgers dan andersom. Een tweede element in de kennisasymmetrie is dat de overheid bovendien ook weet op welke momenten ze wel en niet kijkt. De burger kan er slechts naar raden wanneer iemand in de virtuele wachttoren aanwezig is. Staan de flitscamera’s aan of uit vandaag? Zou er iemand meeluisteren met mijn telefoongesprek? Deze ongelijke kennis is essentieel voor het adequaat functioneren van het disciplinerende mechanisme. Hier fungeert kennis als

machtsmiddel voor de overheid: ‘Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power’ (Foucault, 1979: 303). Degenen die onder surveillance staan, conformeren zich aan de opgelegde normen, omdat ze altijd gecontroleerd kunnen worden. Daarom voor de zekerheid toch maar niet te hard rijden en het woord ‘bomaanslag’ vermijden aan de telefoon. Tegelijkertijd is er sprake van internalisering van normen: degenen die onder surveillance staan maken zich de opgelegde normen eigen en passen haast onmerkbaar hun gedrag hierop aan. Via internalisering komt de disciplinerende macht van het elektronisch superpanopticon tot uiting.

Het technologisch gemedieerde panopticon wordt in de literatuur aangeduid als superpanopticon. Dit heeft te maken met de hoeveelheid en de aard van de kennis die de controlestaat doet functioneren. Informatie- en communicatietechnologie (ICT) stelt de overheid in staat meer en andere kennis over burgers te genereren dan voorheen. Afwijkingen van de norm zijn sneller en gemakkelijker te constateren, omdat surveillance in deze optiek veel verder gaat dan alleen letterlijk ‘toezien op’ (Lyon, 2007b: 450). Tegenwoordig gaat het meer om het verzamelen en interpreteren van data. Ook visuele input zoals foto’s van kentekenplaten wordt nu omgezet in data die via software verder bewerkt kunnen worden (Van Ooijen, 2011). ICT betekent zodoende meer dan een versterking van de zintuigen van de bewaker (een camera ziet en onthoudt meer dan een bewaker). ICT transformeert de zintuigen dankzij de calculatie- en analysefuncties van software. De door de overheid gewenste kennis over burgers, wie op welke manier afwijkt van het normale, kan op meer manieren dan ooit worden verkregen. Het elektronische superpanopticon overschrijdt de traditionele grenzen van plaats, tijd en menselijke waarneming. Niet langer is er één centrale wachttoren, maar zijn er meerdere die met elkaar in verbinding staan dankzij ICT: ‘If the constitution forbids us from spying on our own citizens, never mind, we can get the neighbouring government to do it for us and exchange data’ (Bannister, 2005: 76). Vanuit het controleperspectief betekent surveillance voor burgers dat hun gangen zowel in het heden als het verleden en misschien zelfs de toekomst kunnen worden nagegaan door hun eigen en andere overheden.

4.3 Assumpties over technologie en legitimiteit

Het controleperspectief veronderstelt dat surveillancetechnologie de overheid als kijker de mogelijkheid biedt om de burger als bekeken te controleren op afwijkend gedrag (soevereine macht) en te disciplineren (disciplinerende macht). Een centraal vraagstuk over surveillance vanuit controleperspectief is dan ook hoe de macht van de staat gecontroleerd kan worden. Naast de focus op *checks and balances* ten aanzien van de

staatsmacht verbindt veel literatuur deze machtsvraag aan het recht op privacy van burgers. In de woorden van surveillancetheoreticus David Lyon: ‘in the case of the Orwellian and the panoptic imagery for capturing what surveillance is about, the language of privacy has popular cachet’ (Lyon, 2007b: 460). Dit is bijvoorbeeld te zien in het werk van Bannister:

‘A traditional limitation on the power of the state to invade privacy was that there were many of us and few of them. It seems unlikely that technology will overcome this limitation in the immediate future, but there is no reason, in theory, why it should not. If and when it does, the panoptic state will become a reality.’
(Bannister, 2005: 70)

Vanuit het controleperspectief bestaat dan ook de veronderstelling dat twee maatstaven een rol spelen bij de beoordeling van de legitimiteit van surveillance: het recht op de inzet van het machtsmiddel surveillance en de mate van privacyschending van burgers. Hierbij worden juridische regels, normatieve principes en maatschappelijke steun die surveillance gebieden of toestaan afgewogen tegen legitimiteitsaspecten die de privacy van burgers beschermen.

Of surveillance nu in functie staat van het vergroten van staatsmacht of niet (en de meeste theoretici binnen het controleperspectief denken van wel), essentieel voor het begrijpen van surveillance als controle is dat de relatie tussen ‘kijker’ en ‘bekekene’ gezien wordt als machtsrelatie. Macht is hetgeen dat centraal staat in deze theorievorming, of deze nu meer bij de overheid of meer bij burgers komt te liggen en hoe deze gelegitimeerd kan worden. Om te begrijpen welke invulling de dimensies van de relatie overheid-burger hier krijgen moet dan ook gekeken worden naar mogelijke machtsposities.

4.4 Invulling van de relatie overheid-burger

4.4.1 *Implicaties van het controleperspectief voor de verhouding machthebber-onderdaan*

Wat betekent surveillance – bekeken vanuit het controleperspectief – voor het maken en handhaven van regels (overheid als machthebber), en het kennen en naleven hiervan (burger als onderdaan)? Vanuit het controleperspectief versterkt surveillance de macht van de overheid om bij burgers gewenst gedrag te stimuleren dan wel ongewenst gedrag uit te sluiten. Door hun disciplinerende werking vormen panoptische surveillancesystemen een automatisch handhavingmechanisme dat de naleving van

door de overheid opgestelde regels garandeert. De burger als onderdaan beschikt in het elektronische superpanopticon over twee soorten informatie: kennis van de normen waar hij zich aan dient te houden en de wetenschap dat hij hier altijd en overal op gecontroleerd kan worden. Vanuit het controleperspectief faciliteert en versterkt surveillance door de inherente machtsrelatie tussen kijker en bekeken geruisloos de machtsrelatie tussen overheid en onderdaan. Dit gebeurt op het moment dat de machtspositie van de kijker samenvalt met die van de regelgever en handhaver, en die van de bekeken met die van regelkenner en -nalever. De overheid kan haar regelgeving gemakkelijker en uitgebreider handhaven, omdat surveillancetechnologie de blik van de handhavende functionarissen groter maakt of zelfs vervangt. Tegelijkertijd zorgt surveillance als controle ervoor dat de overheid in feite minder hoeft te handhaven, omdat burgers overheidsregels beter zullen naleven door internalisering hiervan en door de kennis dat ze hierop steeds gemakkelijker gecontroleerd kunnen worden.

4.4.2 Implicaties van het controleperspectief voor de verhouding dienstverlener-cliënt

Wat betekent surveillance – bekeken vanuit het controleperspectief – voor het begrijpelijk, gemakkelijk en toegankelijk maken van diensten (overheid als dienstverlener), en het aanvragen en verkrijgen hiervan (burger als cliënt)? Vanuit het controleperspectief is surveillance vooral van betekenis voor het gemakkelijk en toegankelijk maken van diensten, waarbij de overheid voornamelijk aanbodgericht te werk zal gaan. Het aanbod aan diensten wordt vormgegeven op basis van de gegevens over burgers die de overheid als kijker tot haar beschikking heeft. De beschikbare gegevens stellen de overheid in staat om proactief toegang te verlenen tot haar diensten: ‘volgens onze gegevens verloopt uw paspoort binnenkort; u kunt vanaf heden bij ons terecht voor een nieuw exemplaar’.

Vanuit haar rol als kijker in het elektronisch superpanopticon weet de overheid van alle burgers precies welke diensten op een bepaald moment van toepassing zijn en kan ze hiertoe toegang verlenen en weigeren. Daarnaast kan ze het de burger gemakkelijker maken om een dienst af te nemen, zoals bij de aangifte inkomstenbelasting 2011:

‘U kunt nu gebruikmaken van de vooraf ingevulde aangifte. Dit is een service waarbij wij alvast zo veel mogelijk gegevens invullen in uw digitale aangifte. De gegevens, zoals uw loon en de WOZ-waarde van uw huis, gaan over 2011. Deze gegevens krijgen wij van andere instanties, zoals uw werkgever, uitkeringsinstantie of gemeente. Met deze service willen wij het u zo makkelijk mogelijk maken om aangifte te doen.’

(Belastingdienst, 2012)

Zowel in het toegang geven tot diensten als in het gemakkelijk maken hiervan zijn de surveillancegegevens over burgers het uitgangspunt. Als cliënten hoeven burgers zelf weinig actie te ondernemen om gebruik te maken van de dienstverlening van de overheid. Deze komt vanzelf wel of niet naar hen toe op basis van de gegevens die de overheid over hen heeft. Zodoende worden ze reactieve of zelfs passieve cliënten.

4.4.3 *Implicaties van het controleperspectief voor de verhouding democratisch instituut- citoyen*

Wat betekent surveillance – bekeken vanuit het controleperspectief – voor het representeren, luisteren, betrekken en zich verantwoorden (overheid als democratisch instituut), en het stemmen, initiëren, meepraten en controleren (burger als citoyen)? Op het eerste gezicht lijkt het misschien een contradictio in terminis: een democratische overheid-burgerverhouding in het elektronische superpanopticon. Toch kunnen overheid en burger ook vanuit het controleperspectief zeker wel invulling geven aan de rollen van respectievelijk democratisch instituut en citoyen. Het gaat dan om het aspect van controle/verantwoording van overheidsactiviteiten. Vanuit het controleperspectief heeft de invulling van de citoyenrol betrekking op de vraag in hoeverre en op welke manier burgers zelf surveillance kunnen bedrijven jegens de overheid om daarmee tegenwicht te bieden aan de disciplinerende overheidssurveillance. Deze tegen-surveillance wordt ook wel aangeduid als *sousveillance*: ‘One way to challenge and problematize both surveillance and acquiescence to it is to resituate these technologies of control on individuals, offering panoptic technologies to help them observe those in authority’ (Mann, Nolan en Wellman, 2003: 332). Stevens en de Jong (2010: 155) spreken in dit verband van machtsverhoudingen die zijn omgekeerd en noemen hierbij het voorbeeld uit 2004 van de verspreiding van beelden uit de Abu Ghraib gevangenis waarop lachende soldaten naast gemartelde gevangenen te zien waren. Door *sousveillance* kan de citoyen de transparantie van de overheid vergroten en deze aanzetten tot verantwoording voor de geobserveerde activiteiten.

Hoe surveillance als controle ervaren kan worden door burgers is te lezen in onderstaand imaginair relaas over mevrouw Smit.

4.5 Mevrouw Smit ervaart surveillance als controle

Mevrouw Smit forenst in haar auto elke dag heen en weer tussen huis en werk. Na een lange dag werken stapt ze ook vanavond weer in de auto. Lekker snel naar huis en dan een avondje helemaal niets. Manlief zorgt waarschijnlijk wel voor het eten. Het enige wat zij hoeft te doen is bedenken of ze eerst in bad gaat en daarna Sex and the city gaat kijken of andersom. Haar overpeinzingen worden ruw verstoord door een telefoontje van haar echtgenoot. 'Hoi schat, ik ben wat later...kan jij de kinderen ophalen bij de crèche?'. Mevrouw Smit zucht diep en reageert wat kribbig: 'Dit is al de zoveelste keer! Kan je nou nooit eens een keer op tijd klaar zijn?'. Voordat meneer Smit kan reageren op de tirade van zijn echtgenote schiet mevrouw Smit in de rol van onderdaan en voegt er een beetje aarzelend aan toe: 'Ik bedenk me nu ook dat ik wel eens in de problemen kan komen hierdoor. Ik bedoel, je weet nooit of ze meekijken natuurlijk. Voor hetzelfde geld ben ik er nu bij'. 'Dat zal heus wel meevallen', antwoordt meneer Smit smalend. 'Doe nou maar, dit weekend maak ik het goed'. Toch zit het mevrouw Smit niet helemaal lekker. Als citoyen weet ze van de controles. Ze weet dat de belastingdienst leaseautomobilisten controleert op rijden voor privé-gebruik. Hoe dit precies gebeurt, weet ze niet. Misschien wel met die camera's boven de weg. Een kennisje van de buurvrouw hadden ze met haar leaseauto betrappt bij de IKEA. Ze hadden haar al een tijdje in de gaten gehouden en wisten haarfijn te vertellen dat ze in het afgelopen half jaar vier keer bij IKEA was geweest en een keer bij de Efteling. Toen mevrouw Smit dit verhaal hoorde van de buurvrouw sloeg haar de schrik om het hart. Als ze die kennis konden traceren, moesten ze dat bij haar ook kunnen. De vraag is of ze dat nu ook zouden doen. Als ze nu besluit om voor de vierde keer deze maand van haar woon-werkroute af te wijken en de kinderen op te halen, kan dat wel eens de druppel zijn. Nu ze er zo over nadenkt, valt haar ineens op dat ook boven deze weg camera's hangen. Zouden ze aanstaan? Wat zouden ze precies fotograferen? Waren ze er de vorige keer eigenlijk ook al? O nee, nu rijdt ze ook nog veel te hard. Mevrouw Smit krijgt het gevoel niet te kunnen ontsnappen aan een fikse boete. Gelukkig kan ze er als cliënt van de overheid op vertrouwen dat ze netjes een brief thuis krijgt met alle informatie over haar overtreding overzichtelijk op een rijtje en het verschuldigde bedrag ingevuld op de bijgevoegde acceptgiro. Ze heeft echter geen idee dat ze voor iets veel ergers moet vrezen.

Intussen in het ANPR-datacentrum van het lokale politiekorps is agent Groen druk aan het werk. Tevreden slaat hij de bedrijvigheid om hem heen gade. Het ene na het andere veiligheidsalarm gaat af waar zijn collega's gretig actie op ondernemen. Wat een mooi systeem is het toch en wat is hij trots dat hij hier deel van mag uitmaken. Op zijn

scherm verschijnt een melding 'snelheidsovertreding >50'. Die auto moet straks worden aangehouden. Hij seint een motoragent in en trekt intussen de bewuste auto na in het systeem, zodat bij de aanhouding alle relevante informatie voorhanden is. Hiertoe logt hij eerst in op de database van de Rijksdienst Wegverkeer voor de tenaamstelling bij deze nummerplaat. Vervolgens zoekt hij op naam en nummerplaat in de beschikbare politiedatabases en partnerdatabases. Al snel ziet hij dat het voertuig geregistreerd staat bij een leasemaatschappij en al een aandachtsvestiging heeft van de Belastingdienst. 'Dit zal wel weer een IKEA-klant zijn', denkt Groen. Voordat hij dit kan doorgeven aan de motoragent verschijnt er een code rood op zijn scherm. Hier is dus iets meer aan de hand. Correlatie met woninginbraken?! Hij klikt verder op zijn scherm en ziet een kaartje verschijnen van de regio met daarop de locaties en tijdstippen van acht woninginbraken die afgelopen maand zijn gepleegd. Een tweede en derde data laag op de kaart onthullen dat plaats- en tijdbewegingen van zowel de auto als de gsm van mevrouw Smit hiermee correleren. 'Dit mag ze wel eens komen uitleggen', denkt agent Groen. Snel fluit hij de motoragent terug. Hier is zwaarder geschut nodig. 'Deze dame gaan we binnenkort thuis met een bezoekje vereren' zegt hij triomfantelijk tegen zijn collega.

In het volgende theoretische perspectief op surveillance, het interactieperspectief, laat ik de focus op machtsverhoudingen van het controleperspectief los, waardoor een heel ander beeld van surveillance en haar implicaties voor de relatie overheid-burger ontstaat.

5 Het interactieperspectief

5.1 O burgers, deelt en verbindt uw informatie!

Burgers delen kennis over anderen, maar ook over zichzelf via de datawolken die ze in toenemende mate produceren (Van den Boomen, 2007). Deze observatie staat haaks op het controleperspectief dat een beeld schetst van de burger die geïsoleerd in zijn panopticoncel overheidssurveillance ondergaat. Hierbij is hij onzichtbaar voor andere burgers. Zou de burger in contact staan met andere burgers, dan ontstaat een probleem voor de werking van het panopticon als controlemechanisme en als theoretisch model, want 'this invisibility is a guarantee of order. [...] There is no danger of [...] bad reciprocal influences' (Foucault, 1979: 303). Dat burgers wel degelijk met elkaar in verbinding staan, is een gegeven binnen en een voorwaarde voor democratie. Jürgen Habermas (1974) laat dit duidelijk zien in zijn beroemde verhandeling over *Öffentlichkeit*, de publieke sfeer. De publieke sfeer is een domein in de samenleving waarin burgers zich, gefaciliteerd door massamedia, organiseren om de publieke opinie

vorm te geven. Alle burgers hebben toegang tot de publieke sfeer en genieten de vrijheid om hier hun mening te geven over zaken die het algemeen belang aangaan. Zodoende ontstaat er kritiek op en controle van het handelen van de staat, waardoor de publieke sfeer functioneert als een mediator tussen samenleving en staat. De onderkenning dat er een publieke sfeer bestaat waarin burgers in verbinding staan met elkaar en gezamenlijk interacteren, geeft een fundamenteel ander uitgangspunt voor de bestudering van surveillance dan in het controleperspectief. Haggerty (2006: 27) merkt dan ook terecht op dat ‘changes in surveillance processes and practices are progressively undermining the relevance of the panoptic model for understanding surveillance’. Gefaciliteerd door social media³³ lijkt surveillance onderdeel te zijn geworden van de publieke sfeer en hand in hand te gaan met publieke opinievorming. Social media lijken letterlijk de muren van het panopticon, die de laterale onzichtbaarheid van burgers garandeert, neer te halen. Ze faciliteren wederzijdse beïnvloeding van burgers en tegelijkertijd bestaan social media dankzij deze wederzijdse beïnvloeding. Ondanks dat sommige auteurs (Fuchs, 2011; Fuchs, Boersma, Albrechtslund et al., 2011) laten zien dat surveillance via social media geanalyseerd kan worden vanuit het controleperspectief, leidt de dynamiek van social media naar een ander perspectief met andere vraagstukken. Het interactieperspectief op surveillance ontkent niet dat burgers met elkaar in verbinding staan en elkaar beïnvloeden, maar benadrukt dit gegeven juist.

Hierbij kan de overheid betrokken zijn, maar dat is niet noodzakelijkerwijs het geval. Twee voorbeelden van surveillance van weggedrag in Nederland illustreren dit. Nederlandse burgers kunnen onbehoorlijk weggedrag van medeburgers op verschillende manieren online aan de kaak stellen. Op de website www.asociaalweggedrag.nl kunnen weggebruikers via een formulier melding doen van gedrag als bumperkleven of te hard rijden. Dit formulier komt vervolgens bij de politie terecht. ‘Zij zullen dan deze wegpiraten aanspreken op hun asociale rijgedrag’, aldus de anonieme makers van de website. Van een andere orde is de website www.samenveilig.nl waar burgers via een GIS-applicatie opvallend rijgedrag kunnen melden en tegelijkertijd zien of er een melding over henzelf is gedaan. Op asociaalweggedrag.nl is een duidelijke rol weggelegd voor de politie, zij het een reactieve op basis van meldingen van burgers. Samenveilig.nl gaat met name uit van het zelfcorrigerend vermogen van burgers, zonder tussenkomst van de overheid. Door elkaar via de site, voor het oog van de online gemeenschap, direct aan te spreken op ongewenst rijgedrag moeten burgers gestimuleerd worden op een veilige manier aan het verkeer deel te nemen. Surveillance krijgt zo een wederkerig karakter. Daarnaast

³³ Deze Engelse term is gangbaarder in het Nederlands dan de Nederlandse vertaling ‘sociale media’.

roepen de makers van de website de politie op tot actie naar aanleiding van de verrichte burgersurveillance:

‘De eigenaar van een kenteken dat dagelijks meermaals gemeld wordt voor te hard rijden verdient een vaderlijk gesprek. Of misschien zelfs een signaal aan het CBR dat de rijvaardigheid nog maar eens getoetst moet worden.’

Beide voorbeelden maken duidelijk dat dit type surveillance alleen werkt als er genoeg informatie wordt gegenereerd door en uitgewisseld tussen burgers zelf. De manier waarop vanuit het interactieperspectief surveillance-informatie tot stand komt, volgt de logica van social media.

5.2 De logica van social media

Kaplan en Haenlein (2010, geciteerd in Keymolen, Van den Berg, Prins en Frissen, 2010) omschrijven social media als ‘a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, which allows the creation and exchange of user-generated content’. Social media zijn overigens niet beperkt tot het (mobiele) internet alleen, maar kunnen ook gebruik maken van andere technologieën, zoals het mobiele telefoonnetwerk (Bekkers en Meijer, 2010; Schoondorp, 2010). Benkler (2006: 372-375) heeft het over sociale software en benadert deze vooral vanuit zijn sociale functie. Keymolen et al. vatten de definitie van deze auteur als volgt samen:

‘Eenvoudiger gezegd verwijst de term sociale software naar infrastructuur, internet-omgevingen en applicaties die gebruikers in staat stellen om 1) samen te werken en met elkaar te communiceren in netwerken; 2) relaties aan te gaan en te onderhouden; en – voortvloeiend uit de eerste twee punten – 3) op verschillende manieren sociale aspecten van hun leven in de fysieke wereld in de praktijk te brengen in online omgevingen.’

(Keymolen et al., 2010: 26-27)

Ook Schoondorp (2010: 6) definieert social media aan de hand van hun functie: ‘Social media faciliteren georganiseerde vormen van gezamenlijk acteren’. Het gezamenlijk acteren van gebruikers kan enerzijds gericht zijn op de content (inhoudelijke informatie) op een bepaald platform en anderzijds op het sociale proces dat daar plaatsvindt. Social media die draaien om de co-creatie van informatie worden ook wel collaborative workspaces (collaboratieve werkruimtes) (Keymolen et al., 2010: 27) of object-centered (objectgerichte) social media (Schoondorp, 2010: 8) genoemd. Dit type applicaties draait primair om het creëren, beheren en delen van content die veelal, maar

niet noodzakelijkerwijs in samenwerking tussen gebruikers tot stand komt. Een bekend voorbeeld is Wikipedia, de dynamische online encyclopedie die zijn content ontleent aan de bijdragen van zijn gebruikers. Bij network-centered (Schoondorp 2010: 8) of social networking (Keymolen et al., 2010: 28) sites gaat het niet zozeer om de content die wordt geproduceerd, maar staan menselijke relaties centraal. Volgens Keymolen et al. (2010: 28) stelt dit type social media gebruikers primair in staat 'zichzelf te presenteren aan andere gebruikers van hetzelfde domein, en maakt het hen bovendien mogelijk hun sociale relaties via het netwerk te onderhouden'. Profielsites, zoals bepaalde (mobiele) dating websites, en sociale netwerkanwendungen, zoals Twitter en Facebook, zijn voorbeelden hiervan.

De interactie tussen gebruikers van social media kan dus gericht zijn op het creëren van content of op het aangaan en onderhouden van sociale contacten. Beide vormen van interactie op social media kunnen bedoeld of onbedoeld surveillance faciliteren, die zowel door burgers als door de overheid geïnitieerd kan worden. Een voorbeeld van een burgerinitiatief tot surveillance is het voormalige *meldpuntpedofilie.hyves.nl* waar burgers melding konden maken van pedofiel gedrag bij hen in de buurt en elkaar om advies konden vragen over hoe ze hiermee om moeten gaan. Verder biedt Twitter een grootschalig platform voor surveillance door burgerjournalisten: 'every day in the US, people randomly witnessing an exceptional or dramatic event (crime, protest or accident) use their mobile phone to broadcast real-time information from the field on Twitter [translated by the authors]' (Eudes, 2009 geciteerd in De Longueville, Smith en Luraschi, 2009). De overheid maakt ook zelf gebruik van de mogelijkheden die social media bieden voor surveillancedoeleinden. Zo beschrijven Mitchell, Wolak en Finkelhor (2005) hoe rechercheurs zich online voordoen als minderjarigen om pedofielen op te sporen. Daarnaast zijn er verschillende voorbeelden bekend van hoe autoriteiten social media inzetten om burgers willens en wetens te betrekken bij surveillance van medeburgers (Bekkers en Meijer, 2010; Frissen, Van Staden, Huijboom et al., 2008: 21; Keymolen et al., 2010: 45; Osimo, 2008: 45). Politiek en bestuur spelen daarmee in op het sentiment dat burgers steeds luider en zelfbewuster laten horen via alle kanalen die hen ter beschikking staan. En dat allemaal dankzij het veel geprezen democratisch potentieel van ICT (zie onder meer Edwards, 2005 en Snellen, 2005).

Waar burgers in het controleperspectief als gevangenen in het elektronisch superpanopticon leven, weten ze in het interactieperspectief virtuele bruggen te bouwen. Surveillance als interactie betekent dat er niet alleen verbindingen tussen burgers onderling ontstaan, maar ook tussen burger en overheid. Was de overheid in het controleperspectief onzichtbaar in haar virtuele wachttorens, nu is ze benaderbaar voor de burger. Daarnaast hebben we in het interactieperspectief te maken met een sociaal-expressieve burger die al twitterend en bloggend actief is op sociale

netwerksites of profielpagina's en bovendien altijd bereikbaar is via zijn of haar mobiele telefoon. Dit is de burger die optimaal gebruik wil maken van de mogelijkheden die social media bieden om zich te ontplooien, zichzelf te adverteren, te genieten en sociale verbindingen aan te gaan. Waar in het controleperspectief geen plaats was voor kennisontwikkeling door communicatie tussen burgers en overheid, en burgers onderling, zien we dat dit in het interactieperspectief juist een centrale plek inneemt in de vormgeving van surveillance. Het interactieperspectief benadrukt de democratisering van informatie en van surveillance. Informatie over personen is toegankelijk voor velen, komt tot stand door velen en wordt aangepast en beoordeeld door velen. Surveillance-informatie is wijdverspreid evenals de mogelijkheid om in de rollen van kijker en bekeken bij te dragen aan surveillance. Iedereen kan kijken (naar informatie over anderen) en bekeken worden (op basis van door zichzelf of anderen gedeelde informatie). Het is echter de vraag wat iemand die kijkt daadwerkelijk ziet. Hoe kan user-generated informatie worden gewaardeerd? In de literatuur zijn hierin twee concurrerende posities te ontwaren.

Pessimisten denken dat mensen vanuit een 'infinite desire for personal attention' (Keen, 2007: 7) de grootste onzin zullen delen met de wereld en hierbij niet worden gecorrigeerd door andere aanwezigen in de publieke ruimte: burgers, maar ook de overheid of allerhande experts zoals wetenschappers en journalisten. Ieders mening telt immers. De vrijheid om die mening luid en duidelijk te verkondigen wordt door de sociaal expressieve burger ook als groot goed beschouwd. Het interactieperspectief is doordrenkt van een verregaand waarden- en kennisrelativisme. De enige waarden die breed gevierd lijken te worden hebben betrekking op autonomie en individualiteit. Daarbij lijkt niet de beschikking over kennis, maar het hebben van een mening voldoende voorwaarde om de stem te mogen laten horen.

Optimisten vertrouwen juist op de collectieve intelligentie van de massa gebruikers, 'the wisdom of the crowds' (Surowiecki, 2004) die er altijd voor zal zorgen dat onjuiste informatie gecorrigeerd wordt (Keymolen et al., 2010: 20). De massa selecteert en ordent de enorme hoeveelheden content die ze zelf produceert. Gebruikers zijn 'de enigen die de massale verspreiding van al die nieuwe informatie, content, producten en diensten kunnen filteren op belang, op zinvolheid, op waarheidsgehalte (denk bijvoorbeeld aan Wikipedia), op waarde et cetera' (Keymolen et al., 2010: 22).

5.3 Assumpties over technologie en legitimiteit

Vanuit het interactieperspectief wordt verondersteld dat technologie functioneert als verbinder tussen verschillende actoren in de samenleving. Volgens de logica van social

media creëren en beoordelen allerhande gebruikers informatie over zichzelf en over elkaar. Doordat deze informatie gemakkelijk toegankelijk is voor iedereen, wordt surveillance een aangelegenheid voor iedereen. Surveillancetechnologie stelt zowel overheid als burgers in staat om de rol van kijker aan te nemen en om wat ze zien kenbaar te maken aan iedereen, inclusief de bekekenen. Hierdoor wordt de bekekenen, samen met andere actoren in de samenleving in staat gesteld de betreffende surveillance-informatie te beoordelen, aan te vullen of te corrigeren. Legitimiteit gaat in het interactieperspectief om twee zaken: toegang tot surveillance en de waarde en kwaliteit van surveillance-informatie. Omdat de technologie iedereen faciliteert om als kijker en als bekekenen deel te nemen aan surveillance, werpt dit de vraag op wanneer deze toegang legitiem is. Op basis van welke juridische, ethische en maatschappelijk geaccepteerde gronden krijgt iemand de plicht of het recht om als kijker of bekekenen te participeren in surveillance? Daarnaast is de legitimiteit van surveillance te beoordelen aan de hand van de waarde en kwaliteit van de gegenereerde surveillance-informatie. Welke informatie uit de enorme hoeveelheid geproduceerde user-generated informatie is van belang in een bepaalde surveillancesituatie? Van welke kwaliteit is vervolgens de relevant bevonden informatie? Hoe nauwkeurig en betrouwbaar is deze? Aan de hand van welke juridische, ethische, en maatschappelijke maatstaven kunnen deze zaken worden beoordeeld? Om te begrijpen welke invulling de dimensies van de relatie overheid-burger krijgen in het interactieperspectief moet gekeken worden naar de betekenis van vrije toegang tot surveillance en de waarde van surveillance-informatie.

5.4 Invulling van de relatie overheid-burger

5.4.1 Implicaties van het interactieperspectief voor de verhouding machthebber-onderdaan

Wat betekent surveillance – bekeken vanuit het interactieperspectief – voor het maken en handhaven van regels (overheid als machthebber), en het kennen en naleven hiervan (burger als onderdaan)? Surveillance als interactie zorgt ervoor dat de burger betrokken raakt bij het maken en handhaven van regels. Gewenst en ongewenst gedrag kan door de overheid, maar met name door medeburgers via social media, zichtbaar worden gemaakt. Dit impliceert dat burgers menen in staat te zijn om elkaars gedrag te beoordelen en de plicht of het recht voelen om dit te doen. In sommige gevallen gebeurt dit aan de hand van maatstaven van de overheid, maar er zijn ook situaties waarin medeburgers zelf bepalen wat wel en niet wordt geaccepteerd en vervolgens gerapporteerd. Die surveillerende medeburgers manifesteren zich dan als informele regelgevers en handhavers, waardoor zij machthebbertaken van de overheid aanvullen

of overnemen. De burgers die bekeken worden, worden zodoende aangesproken als onderdanen, terwijl zij hun surveillerende medeburgers niet formeel hebben erkend als machthebber. Hierbij faciliteren deze onderdanen soms deze rol voor zichzelf door informatie over zichzelf te onthullen via social media. Het gedrag van de surveillerende medeburger kan echter behalve als machthebbergedrag ook worden geïnterpreteerd als onderdaangedrag.³⁴ In situaties waarbij de overheid handhavende taken uitbesteedt aan burgers kan dit worden gezien als een beroep doen op danwel de plicht opleggen aan burgers om gewenst surveillerend gedrag te vertonen. In die optiek wordt de overheidspositie van machthebber juist versterkt, omdat de overheid handhaving van regels op grotere schaal kan realiseren dankzij de mens- en technologiekracht van social media.

5.4.2 *Implicaties van het interactieperspectief voor de verhouding dienstverlener-cliënt*

Wat betekent surveillance – bekeken vanuit het interactieperspectief – voor het begrijpelijk, gemakkelijk en toegankelijk maken van diensten (overheid als dienstverlener), en het aanvragen en verkrijgen hiervan (burger als cliënt)? Vanuit het interactieperspectief is het begrijpelijk, gemakkelijk en toegankelijk maken van diensten niet exclusief voorbehouden aan de overheid, omdat zij slechts één van de vele actoren is die dienstverleningsinformatie produceert. De burger heeft een dubbelrol als producent en consument (prosumer) van dienstverleningsinformatie. Als cliënt profiteert hij van surveillance-informatie die door medeburgers is gegenereerd, zoals een misdaadkaart van de buurt waar hij misschien een huis gaat kopen of onthullingen op een online forum over hoe op een ‘creatieve’ manier een vergunning of toelage is verkregen. De interactieve mogelijkheden op de platforms die de cliënt bezoekt, nodigen vervolgens uit om de aangetroffen informatie aan te vullen, te corrigeren of goed te keuren. Vanuit het ideaal van ‘the wisdom of the crowds’ zorgt deze situatie voor passiviteit aan de kant van de overheid. In die optiek zorgen burgers er immers zelf voor dat de juiste dienstverleningsinformatie tot hen komt. Aan de andere kant is het waarschijnlijk dat de cliënt het lastig vindt om de veranderlijke dienstverleningsinformatie op waarde te schatten. De overheid kan in deze als moderator en/of (anonieme) participant fungeren (Bekkers en Meijer, 2010). Reagerend op de informatie die burgers over zichzelf of medeburgers blootgeven, kan de overheid correcties aanbrengen, toelichting geven en passende diensten aanreiken.

³⁴ Maar ook als citoyengedrag, zie 5.4.3.

5.4.3 Implicaties van het interactieperspectief voor de verhouding democratisch instituut-citoyen

Wat betekent surveillance – bekeken vanuit het interactieperspectief – voor het representeren, luisteren, betrekken en zich verantwoorden (overheid als democratisch instituut), en het stemmen, initiëren, meepraten en controleren (burger als citoyen)? De burger kan zich manifesteren als citoyen door surveillance ten aanzien van zijn medeburgers te initiëren of daaraan mee te werken. De informatie die hierdoor gegenereerd wordt, stelt burgers in staat om elkaars gedrag te beoordelen en wenselijk gedrag te stimuleren. Wanneer de publieke ruimte niet verwordt tot een kakofonie aan onsamenvattend lawaai, kunnen burgers zodoende de samenleving zelf mede vorm geven. Dit impliceert dat de surveillerende burger meent het recht te hebben om zich met overheidshandhaving te bemoeien en deze zelfs deels over te nemen. De overheid kan luisteren naar de burger door hem de ruimte te geven tot zelfregulering. Hiermee geeft zij een passieve invulling aan de rol van democratisch instituut. De overheid kan ook de door burgers geuite normen met hen bespreken en meenemen in de vormgeving van overheidshandhaving. In dat geval handelt de overheid in reactie op de onderlinge surveillance tussen burgers.

5.5 Mevrouw Smit ervaart surveillance als interactie

Mevrouw Smit forenst elke dag tussen huis en werk. Ook vandaag stapt ze na een lange werkdag in de auto om op huis aan te gaan. Na het instappen meldt het On-Board-Diagnostics-systeem (OBD) dat de bandenspanning laag is en dat de auto toe is aan een servicebeurt. OBD heeft de data al naar mevrouw Smits vaste garage gestuurd, die haar binnenkort zal bellen om een afspraak te maken. Daarna zet ze de navigatie aan, wacht even totdat haar smartphone contact legt met de radio en rijdt weg zodra de muziek start. Het navigatiesysteem verwacht dat mevrouw Smit over 56 minuten thuis is. Ze heeft tijd genoeg om ondertussen naar huis te bellen. Mevrouw Smit zegt haar telefoon meneer Smit te bellen. 'Hallo schat, hoe is het? Ik ben er over een uurtje. Kook je iets lekkers?' Meneer Smit is verlaat. 'Kun je wel de kinderen ophalen?' Manlief antwoordt ontkennend en zegt dat het nog wel even kan gaan duren. Als mevrouw Smit nu de kids gaat halen, probeert hij wel op tijd het eten op tafel te hebben. Vooruit dan maar. 'Moet ik straks wel de stad door...', denkt mevrouw Smit.

Intussen geniet ze van een nummer – geselecteerd door de online muziekdienst op basis van haar luistergedrag – als de muziek wordt onderbroken. De radio meldt een file bij Rotterdam. Mevrouw Smit kan voorlopig nog doorrijden en trapt het gaspedaal wat dieper in. Ze moet wel om zeven uur bij de crèche zijn, anders krijgt ze daar

problemen. Ze weet dat er geen vaste flitscamera's op dit traject zijn. Daarnaast weet ze dat meldingen van mobiele flitsacties doorgaans snel door andere gebruikers aan haar navigatiesysteem worden toegevoegd. Als cliënt maakt ze gretig gebruik van deze service van haar medeweggebruikers. Uiteraard draagt ze zelf ook zo goed mogelijk haar steentje bij. Misschien had ze wel laatst per abuis die geparkeerde blauwe bus voor een flitsbus aangezien, maar dat kan de beste overkomen, bedenkt mevrouw Smit. 'Bovendien kunnen mensen altijd nog zelf nadenken, toch?' Een sms van meneer Smit haalt haar uit haar overpeinzingen. Het eten gaat voorlopig niet lukken...Inmiddels staat mevrouw Smit toch vast in de file. Ze twittert snel: 'mannen...' en start vervolgens de bezorgthuis-applicatie op haar smartphone. Een overzicht van restaurants die bezorgen in haar postcodegebied verschijnt op het scherm. Natuurlijk wil ze alleen bestellen bij een restaurant met een goede beoordeling. 'Hmm, Italiaans of toch maar iets van de Thai die maar liefst vier smileys heeft gekregen?'

Dan belt haar vriendin Elise. Via de friendfinder-app heeft ze gezien dat mevrouw Smit ook in de file staat. 'Ja, nu zie ik je ook op de friendfinder-map. Je staat wel anderhalve kilometer voor me hoor. Zie je al iets van dat ongeluk? Een ooggetuige twittert net dat één van de bestuurders waarschijnlijk dronken was. Dat is natuurlijk niet toegestaan als onderdaan van ons land! Hij slingerde alle kanten op voordat hij die andere auto raakte. Wel fijn dat sommige mensen hun citoyentaken serieus nemen en dit soort misstanden melden aan ons, medeburgers. Oh het begint alweer te rijden? Gelukkig maar, we spreken snel af voor een avondje Sex and the city of anders zwijmelen bij Mr. Darcy!'. Twintig minuten later is mevrouw Smit ook uit de file en arriveert net op tijd bij de crèche. 'Sorry dat ik wat aan de late kant ben, er zat een of andere dronkenlap op de weg'. Ze zet de kinderen snel achterin. Bij aankomst thuis wordt precies de bestelde maaltijd bezorgd. Mevrouw Smit ploft moe op de bank neer. Even later ziet ze via de mobiele tv op haar telefoon een huilende mevrouw vertellen dat haar man nooit dronken achter het stuur zou kruipen. Hij was onderweg door een hartaanval getroffen. Mevrouw Smit slikt. Ze schaamt zich dat ze de tweet over het dronkenschap zomaar geloofde. Tijdens het tandenpoetsen krijgt ze een berichtje van de verkeersapp op haar smartphone: 'Twee bestuurders vonden uw rijgedrag niet leuk. Eén bestuurder vond uw rijgedrag leuk. Bezoek onze website voor locatie-informatie bij deze meldingen'. Als een goede onderdaan zoekt mevrouw Smit gelijk op wat er nu precies wel en niet werd gewaardeerd in haar rijgedrag vandaag. Dan kan ze het een volgende keer beter doen.

6 Het voorzorgperspectief

6.1 Voorkomen is beter dan genezen

‘Voorkomen is beter dan genezen’ is het adagium van het voorzorgperspectief op surveillance. Binnen de surveillance studies wijzen verschillende auteurs erop dat surveillance in toenemende mate functioneert binnen een samenleving die onheil en ongemak zo veel mogelijk wil voorkomen. Zo presenteren Van Brakel en De Hert (2011) surveillance als integraal onderdeel van politiestrategieën gericht op het voorkomen in plaats van het bestraffen van criminaliteit. Volgens Lyon (2001a) schiet panoptische theorievorming tekort om sociale classificatie van burgers, die samengaat met de inzet van surveillance voor het identificeren van risico’s, te begrijpen. Hoe kan surveillance als onderdeel van de risicosamenleving dan wel begrepen worden? Door surveillance te beschouwen als een facilitator van het voorzorgdenken in plaats van een controlemechanisme of onderdeel van sociale interactie ontstaat een ander beeld van surveillance dan in de twee eerder beschreven perspectieven. Het voorzorgdenken in de risicosamenleving is in de Nederlandse context eerder beschreven en geanalyseerd door onder andere Borgers (2007), Van Gunsteren (2008), Pieterman (2008), Trommel (2009) en de Wetenschappelijke Raad voor het Regeringsbeleid (2008).

Het voorzorgdenken kan worden gekarakteriseerd als product van elementen uit de risicocultuur en schuldcultuur.³⁵ In de schuldcultuur, die tot aan de komst van collectieve arrangementen in de verzorgingsstaat dominant was, speelde individuele verantwoordelijkheid in de tragiek van het leven een centrale rol. Als burger droeg je vooral zelf verantwoordelijkheid voor het voorkomen van onheil en afwenden van ongemak. In de risicocultuur, die vanaf het einde van de negentiende eeuw steeds dominanter aanwezig was met de alsmaar groeiende verzorgingsstaat, was collectivisering een sleutelwoord. Vragen over schuld en verantwoordelijkheid verschoven van het individu naar het maatschappelijk systeem. Daarin werden vooral kosten-batenanalyses gemaakt over risico’s en remedies. Onheil en ongemak waren

³⁵ De schuldcultuur staat in het algemeen bekend als tegenhanger van de schaamtecultuur. In zijn oratie licht Liebrechts (2007: 7) deze tegenstelling toe: ‘[...] de tweedeling schaamtecultuur en schuldcultuur die vooral dankzij het gebruik door de classicus Eric Dodds in zijn *The Greeks and the Irrational* (1951) gemeengoed is geworden, en die door Andreas Kinneging in zijn *Geografie van goed en kwaad* (2005) weer is opgepakt. Dodds gebruikt het begrip schaamtecultuur ter omschrijving van de naar buiten gerichte ethiek van de Grieks-Romeinse oudheid waarin het idee van eer en respect, en de angst voor verlies ervan (wat tot schaamte leidt) centraal stond. Daarentegen is het Christendom een naar binnen gerichte schuldcultuur, omdat hierin de notie van het geweten en van het besef van schuld een centrale rol speelt.’ Deze tegenstelling is echter minder relevant voor de onderhavige bespreking van het voorzorgdenken dan het contrast tussen de schuldcultuur en de risicocultuur.

misschien niet te voorkomen, maar wel te verzekeren. Individuele verantwoordelijkheden werden zo verruild voor allerlei collectieve, vaak publiekelijk afgedwongen, arrangementen die als vangnet fungeerden. Nu het ideaal van de verzorgingsstaat al geruime tijd onder druk staat, lijkt een oriëntatie op voorzorg in de relatie tussen overheid en burger sterk in opkomst. Hierin zijn opnieuw individuele verantwoordelijkheid en schuld belangrijke elementen. Het zijn echter niet zozeer de getroffensten van onheil die laakbaar en verwijtbaar zijn. ‘Burgers hebben geleerd dat het voorkomen van schade niet hun individuele verantwoordelijkheid is’ is’ (Pieterman, 2008: 76). Of het nu gaat om gespecialiseerde ambtenaren, technologiekenners of terrorismedeskundigen, het zijn nu vooral experts die aan de knoppen lijken te draaien van risicodefinitie en -aankpak, en daarmee morele verantwoordelijkheid dragen voor de werking daarvan.

Volgens Borgers (2007) gaat de handelingslogica in de hedendaagse risico-maatschappij uit van een strenge, dwingende interpretatie van het voorzorgbeginsel. Het juridische voorzorgbeginsel, dat een plek heeft in tal van EU-verdragen over met name de bescherming van het milieu en volksgezondheid, is gericht op het voorkomen van reeds bekende en erkende risico’s. In navolging van Pieterman, Hanekamp en Bergkamp (2006: 7) definieert Borgers dit juridische principe als volgt:

‘Het voorzorgsbeginsel houdt, heel algemeen gezegd, in dat wanneer er een dreiging bestaat van ernstige of onomkeerbare schade, een gebrek aan wetenschappelijke zekerheid niet kan gelden als reden voor het achterwege laten of uitstellen van preventieve maatregelen. Die onzekerheid heeft betrekking op het intreden van de schade. Het voorzorgsbeginsel voorkomt dat handelen pas mogelijk wordt wanneer (voldoende of onomstotelijk) vaststaat dat schade zal intreden of reeds is ingetreden.’

(Borgers, 2007: 18)

Een strenge, dwingende interpretatie van het voorzorgprincipe luidt vervolgens:

‘Vanuit een sterke beleving van de dreiging van allerhande risico’s staat de gedachte centraal dat het gevaar een stap voor moet worden gebleven en dat dus preventieve maatregelen moeten worden getroffen, *ook indien niet zeker is of het gevreesde risico zich zal verwezenlijken* [cursivering – CvO].’

(Borgers, 2007: 19)

De WRR (2008) gaat in zijn interpretatie van het voorzorgsbeginsel nog een stap verder dan Borgers. De raad stelt eveneens een moreel imperatief vast voor preventief handelen door de overheid en voegt daaraan toe dat dit handelen niet alleen geldt voor de aankpak van bekende risico’s, maar met name voor het voortijdig opsporen en

waarderen van nog onbekende risico's. Het gecursiveerde deel van bovenstaand citaat kan dan vervangen worden door *ook indien niet zeker is om welke risico's het gaat*. Het is de taak van experts om in de onzekere wereld proactief nieuwe risico's op te sporen en te waarderen. Daarmee wordt het idee van de risicocultuur, waarin overheidsbeleid zich richt op reeds bekende risico's, uitgedaagd. Voorzorg richt zich niet alleen op het voorkomen van redelijkerwijs te verwachten schade (bekende risico's), maar steeds meer op het voorkomen van verrassingen in de vorm van nieuw gevaar (onbekende risico's).

Vanuit het voorzorgperspectief moet de risico-identificatie die door allerhande experts wordt gemaakt boven elke twijfel verheven zijn. 'Met de kennis van nu...' wordt in politiek opzicht bijvoorbeeld een steeds minder houdbaar verweer. Daar kun je geen beleid op formuleren. In de ogen van politici die hunkeren naar geloofwaardigheid maakt zo'n houding de overheid onbetrouwbaar. Wanneer ongemak of onheil onverhoopt toch toeslaat, accepteren politici én burgers bovendien geen excuses meer die zijn gebaseerd op een kosten-batenanalyse van risico's en de beheersing daarvan (zoals in de risicocultuur van de verzorgingsstaat). Elk falen van de experts is in beginsel verwijtbaar. Experts worden verleid meer en meer informatie te verzamelen om daarmee bruikbare kennis te genereren die in ons aller belang is, risico's in de kiem te smoren en een eventuele schuldvraag te kunnen vermijden. Met meer informatie kunnen ze hun rol als expert ook daadwerkelijk invullen. Informatie kan – nee moet – ook in de ogen van de experts steeds gericht en fijnmaziger worden verzameld om effectief en betekenisvol handelen mogelijk te maken.

6.2 Categorisering van burgers

Vanuit het voorzorgperspectief dient surveillance als basis voor interventies. Gegevens worden verzameld, gecategoriseerd en geanalyseerd om beter vooruit te kunnen kijken. Ongemak en onheil moeten niet alleen voorspeld, maar ook voorkomen worden. 'The leading trend, in most sectors, is towards classificatory, pre-emptive surveillance, that tries to simulate and anticipate likely behaviours', aldus Lyon (2001a: 103). In allerlei surveillancepraktijken is deze tendens zichtbaar. Of het nu gaat om een 'verwijsindex risicojongeren' (voorkomen van onder andere kindermishandeling) of om een database met vingerafdrukken van alle Nederlanders met een paspoort (voorkomen van onder meer terrorisme), de wil om te weten en de drang om te interveniëren zijn nooit ver weg. Bij voorzorg gaat het dan niet om het vervolmaken van het panopticon en het disciplineren van de burger, maar om het beschermen of zo goed mogelijk van dienst zijn van de samenleving. Om risico's voor de samenleving inzichtelijk en beheersbaar te maken, is het categoriseren van burgers essentieel. Surveillance faciliteert dit proces

van ‘social sorting’, zo stelt David Lyon in verschillende publicaties (Lyon, 2001b; 2007a; 2007b; 2010).

Wel/geen terrorismerisico, wel/geen frauderisico, wel/geen huiselijk geweldrisico zijn voorbeelden van categorisering en waar een burger aan onderworpen kan worden. Afhankelijk van de specifieke interesse van een organisatie helpt ICT om bepaalde groepen en individuen te identificeren en te isoleren. Lyon (2007b: 460) noemt het voorbeeld van een veiligheidsdienst die data verzamelt over mensen en hun activiteiten, en secundaire analyses uitvoert (van data die eerder door anderen zijn verzameld) ‘to surveil “suspects” who have been previously identified or who fit a particular profile, in the hope of building a fuller picture of such persons, keeping tabs on their movements, and forestalling acts of violence or terror’. Uit voorzorg verdienen dergelijke “risicoburgers” meer surveillanceaandacht dan anderen. ‘Voor uw en mijn veiligheid, de veiligheid van “ons”, is het daarom nodig ze te observeren, te classificeren en eventueel om in te grijpen voordat het kwaad is geschied’, zo stelt Van Gunsteren (2008: 174).

De interventiedrang van de overheid is tenminste deels te begrijpen als een gevolg van een steeds mondiger burger die haar te pas en te onpas ter verantwoording kan roepen en een oordeel uitspreekt over haar geloofwaardigheid. Deze burgers maken zich zorgen over alle risico’s in de samenleving. Van de overheid verwachten en eisen zij soms dat deze maatregelen neemt om risico’s uit te sluiten (WRR, 2008). De dominante positie van de media in het publieke domein maakt het deze groep burgers mogelijk om experts – bestuurders of niet – ter verantwoording te roepen over het vervullen van hun voorzorgopdracht of in elk geval hun geloofwaardigheid in twijfel te trekken. De betrokken experts worden nauwlettend gevolgd. Het oordeel dat burgers, al dan niet via tussenkomst van de media, vellen over situaties en de (geloofwaardigheid van) daarbij betrokken experts, vormt een belangrijk gegeven in het voorzorgperspectief. Burgers roepen experts als het ware ter verantwoording.

In het voorzorgperspectief ontstaat een ongewisse tweedeling tussen risicoburgers en niet-risicoburgers. Niet langer is gelijkheid leidend, maar juist het verschil. Lyon verwoordt dit treffend door te spreken over *de Ander* als surveillanceobject:

‘But the new modes [of citizenship – CvO] [...] tend to single out particular groups for less-than-favorable attention. Such groups may be thought of as Other – those whose existence stands as a warning and as a limit to those currently enjoying full citizenship entitlements, privileges, and rights.’

(Lyon, 2010: 44)

Deze ambiguïteit plaatst de overheid in een ongemakkelijke positie. Het is onmogelijk om de rechten van beide categorieën burgers in gelijke mate te respecteren. De niet-risicoburgers proberen voorzorg ten aanzien van de risicoburgers op de publieke en politieke agenda te krijgen. De risicoburgers op hun beurt, verlangen rechtvaardiging voor de ongelijke behandeling en de gevolgen hiervan. Van Gunsteren (2008: 181) ziet in surveillance als voorzorg een gevaar voor de democratie: ‘Ook risicoburgers zijn burgers. Laten we dan ook als zodanig met ze omgaan’. De vraag is vervolgens hoe surveillance democratisch gelegitimeerd kan worden. Dit is een uiterst lastig vraagstuk. Het profiel van de risicoburger is immers sterk aan verandering onderhevig. Wie vandaag een eisende burger is, kan morgen een risicoburger zijn. Dat immers wordt zeker niet alleen door de eisende burger bepaald, maar is de uitkomst van het samenspel van surveillanceactoren. Paradoxaal genoeg is – anders dan in het controleperspectief – echter geen sprake van een eenzijdige en asymmetrische machtsrelatie tussen burgers en (experts van de) overheid. Zo is de beoordeling van kennis een soms verhitte aangelegenheid.

6.3 Assumpties over technologie en legitimiteit

Het voorzorgperspectief schetst een beeld waarin surveillance wordt beschouwd als een resultante van het samenspel tussen staat, samenleving en technologie binnen een cultuur gericht op het voorkomen van onheil en ongemak. Surveillancetechnologie heeft in dit perspectief een dubbele functie: zowel het identificeren als het beteugelen van risico's. De analyse van bestaande surveillancegegevens met behulp van datamining³⁶ en profiling³⁷ helpt de overheid om nog onbekende risico's te identificeren (Hildebrandt en Gutwirth, 2008). De overheid komt niet alleen steeds verder, maar ook eerder en met de beste bedoelingen achter de (virtuele) voordeur. Het verschijnsel van de pre-cog uit Steven Spielbergs ‘Minority Report’ (2002) lijkt zo steeds minder ver weg.³⁸ Surveillancetechnologie is zodoende te beschouwen als een actor die invloed heeft op de definiëring van risicogroepen door experts en daarmee op de agendering van verdergaande surveillance ten aanzien van de betreffende burgers.

³⁶ Hildebrandt (2008: 18) definieert data mining als volgt: ‘Data mining is a procedure by which large databases are mined by means of algorithms for patterns of correlations between data. These correlations indicate a relation between data, without establishing causes or reasons. What they provide is a kind of prediction, based on past behaviour’.

³⁷ Profiling heeft betrekking op: ‘The assessment of risks and/or opportunities for the data controller (in relation to risks and opportunities concerning the individual subject’ (Hildebrandt, 2008: 20).

³⁸ ‘Storyline Minority Report: In the year 2054 A.D. crime is virtually eliminated from Washington D.C. thanks to an elite law enforcing squad “Precrime”. They use three gifted humans (called “Pre-Cogs”) with special powers to see into the future and predict crimes beforehand.’ (Internet Movie Database, 2002)

Risicoburgers krijgen te maken met de tweede functie van surveillance: het beteugelen van risico's door bepaalde groepen extra in de gaten te houden. Aan de ene kant duidt surveillance als voorzorg op pogingen van de verzorgingsstaat om met de beste bedoelingen grote hoeveelheden informatie te verzamelen over zijn burgers. Aan de andere kant zijn burgers zelfbewust en in staat om voorzichtig het gedrag van de overheid en haar experts te bekritisieren en te beoordelen.

Wat betekenen deze technologieassumpties nu voor de legitimiteitsassumpties in het voorzorgperspectief? Omdat het voorkomen van onheil en ongemak centraal staat, staat of valt de legitimiteit van surveillance met de manier waarop onheil en ongemak worden gedefinieerd. De vaststelling van risicogroepen en de morele verantwoordelijkheid voor de gemaakte keuzes zijn hierbij van belang. Wat er precies voorkomen moet worden en wie hiertoe surveillanceobject moet worden, zijn belangrijke onderwerpen van discussie als het gaat om de legitimiteit van surveillance. Het voorzorgperspectief op surveillance heeft aandacht voor de complexe en wederkerige verhouding tussen overheid en burger in een samenleving vol potentiële risico's. Op welke juridische, ethische en maatschappelijk gewenste gronden worden selecties van burgers gemaakt en welke gevolgen in termen van sociale ongelijkheid, uitsluiting en onterechte inclusie zijn er voor de betreffende groepen? Om te begrijpen welke invulling de dimensies van de relatie overheid-burger krijgen in dit perspectief moet dan ook gekeken worden naar het identificeren van risico's.

6.4 Invulling van de relatie overheid-burger

6.4.1 *Implicaties van het voorzorgperspectief voor de verhouding machthebber-onderdaan*

Wat betekent surveillance – bekeken vanuit het voorzorgperspectief – voor het maken en handhaven van regels (overheid als machthebber), en het kennen en naleven hiervan (burger als onderdaan)? Vanuit een voorzorgperspectief heeft de overheid net als in het controleperspectief een sterke neiging tot interventie, maar heeft hiervoor andere redenen. In tegenstelling tot in het controleperspectief, waar de overheid burgers controleert en disciplineert om de onderlinge machtsrelatie te handhaven, doet zij dit vanuit een voorzorgperspectief om burgers tegen elkaar en tegen zichzelf te beschermen. De overheid wil haar onderdanen responsabiliseren om risico's voor burgers te beheersen en onheil en ongemak voor hen uit te sluiten. Een focus op risicobeheersing impliceert dat regelgeving en handhaving sterk aan verandering onderhevig zijn en worden toegespitst op bepaalde risicogroepen. Voldoet u aan een

combinatie van deze risicovolle kenmerken? Dan wordt u al gauw ‘gevlagd’ in de index en heeft u wellicht wat meer aandacht nodig. De onderdaan komt in een onzekere, haast Kafkaëske positie terecht, omdat de regels waar hij zich aan dient te houden veranderlijk zijn. Bepaald gedrag dat hij dagelijks vertoont, kan opeens als risicovol worden bestempeld door overheid, medeburgers en surveillancetechnologie.

6.4.2 Implicaties van het voorzorgperspectief voor de verhouding dienstverlener-cliënt

Wat betekent surveillance – bekeken vanuit het voorzorgperspectief – voor het begrijpelijk, gemakkelijk en toegankelijk maken van diensten (overheid als dienstverlener), en het aanvragen en verkrijgen hiervan (burger als cliënt)? Kennis van risico’s en risicogroepen in de samenleving zorgt ervoor dat de overheid in haar dienstverlening gericht te werk kan en wil gaan. Bepaalde diensten worden toegankelijk gemaakt voor bepaalde groepen burgers. Afhankelijk van de risicogroep waar de burger toe behoort, ontvangt hij diensten van de overheid. Als roker bijvoorbeeld kan je zomaar gericht gezondheidsadvies of behandelingen ontvangen (Ball, Daniel, Dibb et al., 2010: 117). Door gericht diensten aan te bieden, wil de overheid voorkomen dat risicoburgers schade aanrichten bij zichzelf, de directe omgeving en/of de samenleving als geheel. Publieke dienstverlening is dan ook gericht op het beteugelen van allerhande risico’s. Deze kan variëren van verkeersinformatie voor de forens (risico op files) en sociale begeleiding van een probleemgezin (risico op kindermishandeling) tot ondersteuning van geïsoleerde jongeren (risico op terroristisch handelen).

6.4.3 Implicaties van het voorzorgperspectief voor de verhouding democratisch instituut-citoyen

Wat betekent surveillance – bekeken vanuit het voorzorgperspectief – voor het representeren, luisteren, betrekken en zich verantwoorden (overheid als democratisch instituut), en het stemmen, initiëren, meepraten en controleren (burger als citoyen)? De overheid luistert naar de burger en geeft deze een stem in beleidsontwikkeling op het moment dat hij zich opstelt als medevaststeller van risico’s en risicogroepen. Als citoyen verlangt de burger openlijk dat de overheid uit voorzorg adequate maatregelen treft om de door hem geïdentificeerde risico’s te beteugelen. Er is gerede kans dat de overheid gehoor geeft aan de dwingende suggesties van de burger of deze tenminste in overweging neemt om te voorkomen dat zij zich later publiekelijk zal moeten verantwoorden als er onheil of ongemak optreedt. Verder is de burger als citoyen (via de media) actief in de beoordeling van bestaande voorzorgarrangementen. Bij de

verantwoording over het gemaakte beleid kunnen surveillancegegevens een belangrijke rol vervullen. De overheid kan zich beroepen op de uitkomst van risicoanalyses via datamining en profiling als grond voor getroffen maatregelen.

6.5 Mevrouw Smit ervaart surveillance als voorzorg

Mevrouw Smit forenst in haar auto elke dag heen en weer tussen huis en werk. Na het instappen navigatie aan en rijden maar. Het navigatiesysteem verwacht dat mevrouw Smit over 56 minuten thuis is. Eerst maar even bellen. Mevrouw Smit zegt haar telefoon meneer Smit te bellen 'Hallo schat, hoe is het? Ik ben er over een uurtje. Kook je iets lekkers?' Meneer Smit is verlaat. 'Kun je wel de kinderen ophalen?' Meneer Smit antwoordt ontkennend en zegt dat het nog wel even kan gaan duren. Als mevrouw Smit nu de kids gaat halen, probeert meneer Smit wel op tijd het eten op tafel te hebben. Vooruit dan maar. 'Moet ik straks wel de stad door...', denkt mevrouw Smit.

Zonder tussenkomst van mevrouw Smit registreert het ritregistratiesysteem in de auto vanzelf de kleine omweg. De administratie zal automatisch worden bijgewerkt. Het systeem zendt alle ritgegevens naar de leasemaatschappij in een format dat ook de belastingdienst kan bekoren. Op de radio verhaalt de directeur van het centrum infectiebestrijding van het RIVM over het feit dat de griep prik echt geen kwaad kan. Een grondige en grootschalige analyse laat dat volgens hem ook zien. 'Tot begin februari werden meer dan 36 miljoen Europeanen gevaccineerd. 155 sterfgevallen werden daarbij aanvankelijk gemeld. Slechts vier bleken uiteindelijk niet te herleiden tot een andere oorzaak. In alle andere gevallen werd een duidelijke andere oorzaak gevonden of speelden onderliggende ziekten of ouderdom een rol. En let wel: historische cijfers wijzen uit dat van die 36 miljoen gevaccineerden er iedere dag sowieso 1000 zouden zijn gestorven'. 'Hmm', denkt mevrouw Smit als een goede, kritische citoyen, 'ik kan het niet helemaal volgen, maar laatst was die meneer ook bij Pauw en Witteman en maakte daar een onzekere en defensieve indruk. Hij werd flink door de mangel gehaald. Daarbij is het natuurlijk idioot dat mensen bezwijken aan een vaccin dat juist zou moeten voorkomen dat ze ziek worden. Ieder sterfgeval is er één te veel! Deze man moet hiervoor aansprakelijk worden gesteld. Ik kan dat vaccin maar beter niet nemen.'

Het navigatiesysteem meldt dat de route wordt aangepast aan de actuele verkeerssituatie. Uit de telefoonsignalen van andere gebruikers en de dynamische snelheidsaanduidingen op de weg van Rijkswaterstaat maakt het navigatiesysteem op dat het verderop al een tijdje stil staat. 'Hmm mooi, maar de file op de A20 bij Rotterdam is vast niet te vermijden...'. So far so good, voorlopig rijdt het lekker door.

De radio meldt dat uit onderzoek blijkt dat auto's van het merk 'klein en schattig' van alle automerken het vaakst betrokken zijn bij botsingen en dat de betrokken bestuurders overwegend blauwogig zijn. De minister van infrastructuur geeft in een reactie aan 'voor alle onderdanen passende maatregelen te hebben getroffen'. 'Elise heeft blauwe ogen...Nee, dat is een te idiote gedachte dat dat iets te maken heeft met de weigering van de bank om zo'n auto voor haar te financieren. Wel raar dat ze zeiden dat het geen goede investering was "in haar situatie"...' peinst mevrouw Smit. Tussen Ridderkerk en de Van Brienenoordbrug wordt de kentekenplaat van mevrouw Smits auto gescand door Rijkswaterstaat. Op basis van eerdere scans voorspelt het computersysteem van deze instantie dat ze de A20 bij afrit 14 zal verlaten. Met de huidige drukte op de weg zouden mevrouw Smit en 268 andere auto's de afrit over zeven minuten moeten bereiken. Daarmee ontstaat het risico op een verkeersopstopping. De dynamische maximum snelheid op de A20 en de afstelling van de verkeerslichten aan het eind van de afrit worden hierop aangepast. Automobilisten worden via hun navigatiesystemen alternatieve routes op gestuurd. De verkeersopstopping wordt voorkomen. Het navigatiesysteem van mevrouw Smit heeft haar uit voorzorg de A15 op geleid. Ze kan gewoon doorrijden en zal de crèche op tijd bereiken. 'Wat een service van Rijkswaterstaat; zo hoor je cliënten te behandelen', denkt mevrouw Smit.

7 Conclusie: theoretische implicaties van surveillance voor de relatie overheid-burger

Dit hoofdstuk laat zien dat de drie perspectieven op surveillance, controle, interactie en voorzorg, verschillende beelden geven van de aard van de surveillancerelatie tussen overheid en burger. Surveillance heeft vanuit ieder perspectief andere kenmerken en daarmee verschillende implicaties voor de relatie overheid-burger. De perspectieven behelzen zowel assumpties over technologie (beleidsmogelijkheden) als over legitimiteit (beoordelingsmaatstaven). Vanuit het controleperspectief is de vraag hoe de inzet van panoptische surveillance, die burgers controleert en disciplineert versus de bescherming van privacy gelegitimeerd wordt. Het interactieperspectief, dat surveillance presenteert als verbinder tussen verschillende actoren in de samenleving, richt zich op de vraag hoe toegang tot surveillance en een bepaalde waarde en kwaliteit van informatie gelegitimeerd kunnen worden. Het voorzorgperspectief veronderstelt dat surveillancetechnologie risico's kan helpen identificeren en beteugelen. Bij legitimiteit in dit perspectief gaat het dan ook om het beoordelen van de gronden waarop risico's en categorieën van burgers worden gedefinieerd.

In lijn met de analyse van literatuur over ICT en democratie van de hand van Van de Donk en Tops (1992) kan geconcludeerd worden dat zowel een verticaal als een horizontaal perspectief aanwezig is. Onderzoekers die een verticaal perspectief hanteren concentreren zich met name op de machtsrelatie tussen overheid en burger. Dit perspectief is terug te zien in het controleperspectief. Literatuur vanuit het horizontale perspectief vormt een reactie op de 'eenzijdigheid van de verticale literatuur' aldus Van de Donk en Tops (1992: 62). Deze tweede lijn in de literatuur legt de nadruk op het proces van deliberatie tussen burgers en hun verbanden onderling. Dit komt terug in het interactieperspectief, dat wetenschappelijk probeert te ontkomen aan het panopticon. Het voorzorgperspectief tenslotte problematiseert niet zozeer de machtsrelatie tussen overheid en burgers of het proces van deliberatie tussen burgers onderling, maar begrijpt het initiatief, het verloop en de uitkomst van surveillance als afhankelijk van verschillende voorzorgcontexten met menselijke en niet-menselijke actoren. Tabel 5 vat de kenmerken van ieder perspectief samen.

In het volgende hoofdstuk, dat over de aanpak van het empirisch onderzoek gaat, werk ik de theorie uit dit hoofdstuk uit tot een analytisch kader, aan de hand waarvan de surveillanceperspectieven in twee Nederlandse beleidspraktijken in beeld worden gebracht.

SURVEILLANCE-PERSPECTIEF	RELATIE OVERHEID-BURGER		
	<i>Machthebber - Onderdaan</i>	<i>Dienstverlener - Cliënt</i>	<i>Democratisch instituut - Citoyen</i>
Controle <i>Macht en privacy</i>	Surveillance faciliteert en vervangt overheidshandhaving van regelgeving.	De overheid verleent toegang tot en gemak bij publieke dienstverlening op basis van surveillancegegevens over burgers.	Door sousveillance maken burgers overheidssurveillance transparant.
	Panoptische disciplinerende zorgt ervoor dat burgers overheidsregels naleven.	Alle burgers worden reactieve of passieve cliënten.	Sousveillance zet de overheid aan tot verantwoording over de surveillance van burgers.
Interactie <i>Vrije toegang tot surveillance en kwaliteit van informatie</i>	Overheidsregelgeving en -handhaving worden aangevuld door burgernormen en -handhaving.	De overheid wordt een passieve, modererende en reagerende dienstverlener.	Surveillance faciliteert zelfsturing en coöperatie met de overheid.
	Overheid en burgers stimuleren medeburgers om mee te werken aan handhaving.	Burgers vervangen door prosumptie van surveillance-informatie voor een groot deel de overheidsdienstverlening.	Burgers eisen een actieve rol op in de handhaving van medeburgers.
Voorzorg <i>Definiëring van risico's en (groepen) risicoburgers</i>	Overheidsregelgeving en -handhaving veranderen snel en richten zich op risicogroepen.	De overheid biedt dienstverlening selectief en proactief aan afhankelijk van groepskenmerken.	Risicoanalyses staan centraal in de verantwoording van beleidskeuzes.
	Burgers verkeren in Kafkaëske onzekerheid door beperkte kennis over veranderlijke normen.	Bepaalde groepen burgers worden reactieve of passieve cliënten.	Risico's op de publieke agenda bereiken gemakkelijk de surveillance-agenda van de overheid.

Tabel 5: Surveillanceperspectieven en de relatie overheid-burger

DEEL II

PUBLIEKE MOBILITEITSSURVEILLANCE IN DE PRAKTIJK

HOOFDSTUK 5

AANPAK EMPIRISCH ONDERZOEK

1 Inleiding

In het literatuuronderzoek in de vorige hoofdstukken heb ik laten zien dat publieke mobiliteitssurveillance een veelzijdig fenomeen is met een rijke politiek-bestuurlijke historie en verschillende verschijningsvormen qua technologie en beleid. Hoe publieke mobiliteitssurveillance zich in de praktijk van het openbaar bestuur manifesteert, en welke implicaties voor de relatie overheid-burger ze dan heeft, hangt af van de beleidsmatige (on)mogelijkheden die beleidsmakers zien met betrekking tot de technologie. Beleidsinterpretaties geven de praktijk van publieke mobiliteits-surveillance vorm. Hoofdstuk 4 heeft duidelijk gemaakt dat surveillance op meerdere manieren bekeken kan worden en dat implicaties voor de relatie overheid-burger naar verwachting sterk verschillen afhankelijk van het gehanteerde perspectief. In het empirisch deel van dit proefschrift, waarvoor dit hoofdstuk de opmaat vormt, beschrijf en analyseer ik de manier waarop beleidsmakers in twee casussen van publieke mobiliteitssurveillance betekenis construeren over de (on)mogelijkheden van surveillancetechnologie. Eén casestudy richt zich op automatische nummerplaat-herkenning (ANPR) bij een politiekorps en de andere betreft het innovatiebeleid van de Nationale Databank Wegverkeersgegevens voor de inwinning en verwerking van wegverkeersgegevens. De twee casusonderzoeken laten zien hoe beleidsinterpretaties van technologie en legitimiteit richting geven aan de daadwerkelijke inzet van bepaalde technologie(ën) ten behoeve van publieke mobiliteitssurveillance. In de komende hoofdstukken beschrijf en analyseer ik de beleidsontwikkeling in de twee casussen van publieke mobiliteitssurveillance en werk ik toe naar een begrip van de implicaties van de aan het beleid onderliggende assumpties over technologie en legitimiteit voor de relatie overheid-burger.

De theoretische hoofdstukken demonstreren dat surveillance in het algemeen – en publieke mobiliteitssurveillance in het bijzonder – op verschillende punten ambiguïteit tentoonspreidt. Mobiliteitsinformatie kan op meerdere manieren worden geïnterpreteerd (hoofdstuk 2) en past zowel bij een voortzetting van politiek-bestuurlijk gebaande paden als een zich razendsnel ontwikkelend technologisch fenomeen (hoofdstuk 3). Daarnaast kan surveillance op hoofdlijnen vanuit drie perspectieven worden geïnterpreteerd, die ieder andere technologie- en legitimiteitsassumpties laten zien (hoofdstuk 4). De ambiguïteit van publieke mobiliteitssurveillance kan voor spanningen zorgen in de beleidsvorming. Wanneer beleidsmakers verschillende

surveillanceperspectieven hanteren, hebben ze immers verschillende ideeën over wat technologie kan betekenen in beleid (technologieassumpties) en welke criteria van belang zijn voor een legitieme inzet van de technologie (legitimiteitsassumpties). In de theoretische hoofdstukken heb ik verwachtingen geformuleerd over de invulling van de relatie overheid-burger bij de drie surveillanceperspectieven controle, interactie en voorzorg. De analyse van de casussen kan uitwijzen op welke punten deze verwachtingen houdbaar zijn in het geval van publieke mobiliteitssurveillance en biedt de mogelijkheid het theoretisch kader aan te passen. Om de implicaties van de in de casussen aanwezige surveillanceperspectieven voor de relatie overheid-burger in beeld te brengen, voer ik een interpretatief beleidsonderzoek uit. In de volgende paragraaf licht ik toe welke methodologie bij dit type onderzoek hoort en welke bronnen en methoden ik heb gebruikt om onderzoeksgegevens te genereren. Hierbij ga ik in op de aard van casusonderzoek volgens een interpretatieve methodologie en de keuze voor de twee casussen in dit onderzoek. Tenslotte bespreek ik in welke stappen ik kom tot een analyse van de onderzoeksgegevens.

2 Methodologie, onderzoeksbronnen en methoden

2.1 Methodologie: niet verklaren, maar begrijpen

In dit onderzoek richt ik mij op het begrijpen van de totstandkoming van publieke mobiliteitssurveillance en wat de manier waarop dit gebeurt betekent voor de relatie tussen overheid en burger. Hiertoe analyseer ik hoe beleidsactoren technologische en legitimitetsmogelijkheden interpreteren. Omdat ik mij bezighoud met betekenisgeving in beleid is in dit onderzoek sprake van een interpretatieve methodologie. In hun artikel in *Public Administration Review* over methodologie en methoden binnen de bestuurskunde leggen Haverland en Yanow de interpretatieve onderzoekslogica als volgt uit:

‘Interpretive researchers hold that knowledge of or ideas about social realities are intersubjectively (or “socially”) constructed and that research-related knowledge can only be developed in interaction with actors in their own settings and situations; “objectivity” – knowing from the outside – is, in this view, not possible.’

(Haverland en Yanow, 2012: 404)

Zoals wel vaker bij een interpretatieve methodologie, is in dit onderzoek sprake van een dubbele heuristiek. De eerste heuristiek is het proces van betekenisgeving door de beleidsactoren die betrokken zijn bij publieke mobiliteitssurveillance. Bij het maken van beleid, zowel tijdens het schrijven van beleidsdocumenten, het vergaderen met

andere beleidsactoren als gedurende andere ontmoetingen, interpreteren beleidsactoren surveillancetechnologie op een bepaalde manier. Hun percepties van wat een bepaalde technologie inhoudt en beleidsmatig kan betekenen, is cruciaal voor de verdere ontwikkeling van het beleid. Vervolgens geef ik als onderzoeker aan de hand van het theoretisch kader een interpretatie van de interpretaties van beleidsactoren. Dit zingevingsproces door de onderzoeker wordt ook wel de tweede heuristiek genoemd. Vanwege de dubbele heuristiek is er sprake van het genereren van onderzoeksgegevens in plaats van verzamelen. De onderzoeksgegevens worden immers geconstrueerd binnen een bepaalde context en niet kant-en-klaar ‘gevonden’ (2007). De methodologie van een onderzoek ligt aan de basis van de keuze voor bepaalde onderzoeksmethoden. Omdat ik wil *begrijpen* wat publieke mobiliteitssurveillance impliceert voor de relatie overheid-burger, kies ik voor onderzoeksmethoden die de mogelijkheid bieden om een zo compleet mogelijk beeld te verkrijgen van de hierbij horende beleidscontext: observatie, documentanalyse en kwalitatieve interviews in casusonderzoek. Casusonderzoek staat mij toe om mij onder te dompelen in een beleidscontext en de praktijk aldaar gedetailleerd in beeld te brengen. Dit type casusonderzoek dient niet verward te worden met casusonderzoek vanuit een positivistische methodologie. De twee onderzoekslogica’s gaan uit van verschillende epistemologische en ontologische opvattingen en zijn dan ook aan andere wetenschappelijke criteria onderhevig (Yanow en Haverland, 2012). Het empirisch onderzoek richt zich op twee beleidspraktijken van publieke mobiliteitssurveillance: ANPR bij een Nederlands politiekorps en de inwinning van verkeersgegevens bij de Nationale Databank Wegverkeersgegevens (NDW).

2.2 Onderzoeksbronnen in twee casusonderzoeken

Het empirisch onderzoek vindt plaats bij twee publieke uitvoeringsorganisaties. Als eerste casus staat een politiekorps³⁹ centraal, dat uitvoerder is van nationaal en lokaal veiligheidsbeleid. De tweede casestudy draait om de Nationale Databank Wegverkeersgegevens, die formeel onderdeel is van Rijkswaterstaat, de uitvoeringsorganisatie voor verkeers- en mobiliteitsbeleid. Ook al zijn het politiekorps en NDW in formele zin uitvoeringsorganisaties, dat betekent niet dat zij beleid blind uitvoeren en zelf geen invloed hebben op de richting en invulling daarvan. Integendeel, de keuze voor publieke uitvoeringsorganisaties als onderzoeksobject is juist gemaakt vanuit de overtuiging dat beleid grotendeels in deze organisaties wordt gemaakt. Deze visie op beleid is enerzijds te motiveren vanuit het idee van beleidsvrijheid en anderzijds vanuit

³⁹ Dit betreft één van de 26 Nederlandse politiekorpsen die bestonden vóór de invoering van de Nationale Politie op 1 januari 2013.

het idee van bottom-up beleidsvorming. Het idee van beleidsvrijheid kennen we in de bestuurskundige literatuur vooral van Lipsky's onderzoek naar street-level bureaucrats (Lipsky, 1980). Beleidsvrijheid, ofwel discretionaire ruimte betreft de ruimte die geformuleerd beleid laat bij de invulling daarvan. De contouren van beleid zijn bekend, maar de situatiespecifieke omstandigheden van de uitvoering zijn niet doordacht door de opstellers van het beleid. Daarnaast beschouw ik beleidsvorming als een alineaar proces waarin de formele besluitvorming op managementniveau en alledaagse beslissingen op de werkvloer elkaar beïnvloeden. Dit wordt ook wel een bottom-up benadering van beleid genoemd waarbij beleidsimplementatie gezien wordt als onderdeel van de beleidsvorming in plaats van een apart proces (Hill, 2009: 202-204). Om die reden bestudeer ik in de twee casussen zowel formele besluiten als operationele ervaringen met surveillancetechnologie. Deze methodologische keuze is niet alleen gebaseerd op theorie, maar heeft tevens een empirisch fundament. Zoals een van de informanten in de politiecasus het verwoordt: *'De politie is heel erg een doe-organisatie die wel eens te weinig nadenkt. Door dingen in de praktijk te laten gebeuren weet ze echter wel de denkers te stimuleren.'*

De twee casussen zijn gekozen, omdat ze zich afspelen in uiterst verschillende beleidsdomeinen waarbij de beleidsdoelen die beide organisaties nastreven met het in beeld brengen van bewegingen van burgers op het eerst gezicht totaal verschillend lijken te zijn. De politiecasus speelt zich af in het veiligheidsdomein, de NDW-casus op het gebied van verkeersmanagement. David Lyons observatie dat surveillance vanuit een behoefte aan *care* of *control* vormgegeven kan worden, lijkt ondersteund te worden bij een eerste blik op de twee casussen. Bij de politie lijkt surveillance 'control' (van overtreders en criminelen) als doel te hebben, en bij NDW 'care' (voor weggebruikers). De eerste casestudy is het verhaal van een Nederlands politiekorps dat al enige jaren ervaring heeft met het gebruik van ANPR en stappen begint te zetten richting nieuwe toepassingen van de technologie rond de tijd dat ik bij hen onderzoek kan doen. Het is dan september 2008 en ik blijf dit politiekorps tot april 2009 actief volgen. De tweede casestudy is het verhaal van een jonge uitvoeringsorganisatie op het gebied van verkeersbeleid, die vanuit politiek Den Haag de opdracht meekrijgt met innovatieve technieken verkeersgegevens te gaan inwinnen. Mijn veldonderzoek bij NDW begint op het moment dat deze organisatie samen met haar grootste partner Rijkswaterstaat in een aanbestedingstraject voor de regio Noord- en Oost-Nederland de zoektocht naar geschikte, nieuwe technologie aangaat. Van december 2009 tot en met oktober 2010 volg ik dit beleidstraject.

Om het beleid in de twee casussen zichtbaar te maken, genereer ik onderzoeksgegevens via observatie, kwalitatieve interviews en documentanalyse. De keuze voor informanten en documenten, ontstaat bij beide casussen gaandeweg het veldonderzoek.

2.3 Technieken voor het genereren van onderzoeksgegevens

2.3.1 *Onderzoeksbronnen genereren onderzoeksbronnen*

In beide casusonderzoeken maak ik een onderscheid tussen sleutelinformanten en overige informanten. Sleutelinformanten zijn de beleidsactoren met wie ik gedurende het veldonderzoek vaker en uitgebreider contact heb dan met andere informanten. Zij fungeren als mijn aanspreekpunten binnen de twee uitvoeringsorganisaties. Bovendien wijzen de sleutelinformanten mij op nieuwe relevante informatiebronnen voor mijn onderzoek. Zodoende zijn de sleutelinformanten de nodes in mijn netwerk van informanten, documenten en beleidsgebeurtenissen.

In de politiecasus zijn er drie sleutelinformanten. Twee van hen werken als beleidsadviseurs bij de dienst die verantwoordelijk is voor de beleidsontwikkeling betreffende ICT. Vanachter mijn eigen bureau op hun kantoor ben ik in staat om telefoongesprekken mee te krijgen en conversaties met collega's te horen en hieraan deel te nemen. Bovendien informeren de twee sleutelinformanten mij actief over beleidsontwikkelingen die plaatsvinden op de dagen dat ik niet aanwezig ben. De derde sleutelinformant werkt op operationeel niveau. Hij leidt de divisie die verantwoordelijk is voor het managen van alle ANPR-data. Alle verzoeken om ANPR-gegevens van binnen en buiten het korps worden door deze ANPR-divisie afgehandeld. Zodoende is deze sleutelinformant in staat om mij ruimschoots te voorzien van informatie over de praktijk van ANPR.

In de NDW-casus zijn er ook drie sleutelinformanten. Twee van hen spelen een centrale rol in de projectgroep en de stuurgroep die betrokken zijn bij de besluitvorming rondom de inwinning van verkeersgegevens in Noord- en Oost-Nederland. De derde sleutelinformant is onderdeel van de NDW-top. Deze persoon heeft het besluitvormingstraject in gang gezet en blijft hier als stuurgroeplid bij betrokken. Daarnaast geeft deze mij inzicht in de bredere beleidscontext van NDW.

In beide casusonderzoeken zijn het steeds de beleidsactoren zelf die mij op het spoor zetten van verdere relevante gesprekspartners en documenten. In een sneeuwbalproces vraag ik iedere informant of hij/zij mij een andere persoon kan aanraden om mee in gesprek te gaan. Dit proces start ik op bij de sleutelinformanten en zet ik door totdat ik het gevoel krijg geen substantieel nieuwe onderzoeksinformatie meer te verkrijgen. De 'sneeuwbal' stopt uiteraard ook wel eens op het moment dat ik geen respons krijg op mijn verzoek voor een afspraak. De onderzoeksgegevens genereer ik door middel van observatie van en interviews met informanten, en via documentonderzoek.

2.3.2 Observatie

Casus ANPR politie

Door meerdere werkdagen op kantoor met twee sleutelinformanten door te brengen, ben ik in staat om hen te schaduwen.⁴⁰ Om praktische redenen plan ik deze dagen op dezelfde dagen als ik interviews kan afspreken. Door mijn aanwezigheid op kantoor kan ik meedoen met de dagelijkse gesprekken tussen mensen op de werkvloer, waardoor ik een goed beeld krijg van de lopende beleidsonderwerpen betreffende ANPR. Ik maak veldnotities van iedere conversatie die ik heb en elke discussie die ik opvang. Als toevoeging op deze dagen op kantoor laat mijn derde sleutelinformant mij verschillende malen de ANPR-software bekijken. Hij bespreekt de belangrijkste query-opties (zoekopdrachten) en beantwoordt mijn vragen over hoe het systeem werkt, welke toepassingen er zijn in politiewerk en aan welke toepassingen wordt gewerkt. Daarnaast kom ik twee keer op één van de centrale locaties in de politieregio waar ANPR-data worden verzameld. Aldaar zie ik de cameraposities, verkeersstromen en de van buiten onopvallende camerabus van waaruit data aan het softwaresysteem worden toegevoegd.

Casus verkeersgegevens NDW

In deze casestudy woon ik verschillende vergaderingen van de projectgroep, stuurgroep en tenderboard bij, waarin ik de gesprekken tussen en het gedrag van de aanwezigen observeer. Daarnaast woon ik verschillende gesprekken bij tussen één van mijn sleutelinformanten en actoren in het bedrijfsleven, de zogenaamde marktconsultaties. Ook ga ik een dag met mijn sleutelinformanten mee naar Intertraffic, een grote internationale vakbeurs voor verkeersspecialisten. Hier ben ik aanwezig op een informatiebijeenkomst van NDW voor de potentiële aanbieders van de gezochte technologie en ben ik getuige van welke beleidsposities NDW presenteert en waarover discussie ontstaat.

⁴⁰ Over 'shadowing' als onderzoeksmethode zie Geuijen, 't Hart en Yesilkagit (2007: 132).

2.3.3 Interviews

Casus ANPR politie

In toevoeging op de spontane, soms uitgebreide gesprekken op de werkvloer zijn met twaalf informanten semigestructureerde interviews gehouden. Van alle interviews op één na heb ik geluidsopnames gemaakt en deze getranscribeerd. Bij één interview blijkt de geluidsopname naderhand niet te zijn gelukt. Ik ontdek dit meteen na het interview en werk het interview onmiddellijk op basis van mijn aantekeningen en directe herinnering uit. Zeven interviews vinden plaats met medewerkers van het politiekorps. De overige vijf informanten betreffen vertegenwoordigers van landelijke politieorganisaties en het lokale Openbaar Ministerie. De lokale politie-informanten vraag ik te vertellen over hun betrokkenheid bij ANPR en de door hen ervaren successen en problemen. De overige informanten verstrekken informatie over de beleidscontext en verhalen over hun ervaringen met het politiekorps betreffende ANPR. Het interviewprotocol (Bijlage I) bestaat uit open vragen, waarbij ruimte is om ter plekke vragen toe te spitsen op de specifieke interviewsituatie.

Casus verkeersgegevens NDW

Ook in deze casestudy houd ik verschillende conversatiestijlinterviews, bij de koffieautomaat of in de auto, waar ik nadien notities van maak. Daarnaast houd ik zeven semigestructureerde interviews om door te vragen op de indrukken die ik opdoe tijdens alle overleggen. Ook in deze casus bestaat het interviewprotocol uit open vragen, waarbij ruimte is om ter plekke vragen toe te spitsen op de specifieke interviewsituatie (Bijlage II). Van deze interviews maak ik geluidsopnames die ik naderhand transcribeer.

2.3.4 Documentonderzoek

Casus ANPR politie

Beleidsdocumenten, werkinstructies, interne (memo's, intranetberichten, e-mails) en externe communicatie (brieven, krantenberichten, presentaties) zijn bestudeerd.

Casus verkeersgegevens NDW

Van alle projectgroep-, stuurgroep- en tenderboardoverleggen maken de twee sleutelinformanten overlegverslagen, die ik doorgaans vanzelf toegestuurd krijg. Deze

verslagen stellen mij in staat om mijn notities van de overleggen te vergelijken met de punten die volgens de sleutelinformanten belangrijk genoeg waren om in verslagen vastgelegd te worden. Naast overlegverslagen maak ik gebruik van beleidsdocumenten van de website van NDW, interne e-mails en van de aanbestedingsdocumenten die de projectgroep vervaardigt.

2.4 Positie van de onderzoeker

Passend bij de interpretatieve methodologie heb ik niet de illusie noch de intentie om als onderzoeker de rol van onzichtbare en neutrale observator te vervullen. De rol van de onderzoeker is juist van belang voor het genereren van onderzoeksgegevens, zo stellen Haverland en Yanow (2012: 404): ‘As a form of explanation, interpretive science’s emphasis is on contextualized meaning making, including not only that of situational actors but also of the researcher, who is also situated or “positioned.”’ Enige beïnvloeding van het te bestuderen proces is derhalve niet te voorkomen, maar moet ook niet worden overschat. Ook al ben ik in beide casusonderzoeken zichtbaar aanwezig op de werkvloer, ik tracht het verloop van de beleidsprocessen niet al te zeer te beïnvloeden. Evenwel kost het me soms moeite om me niet in discussies te mengen en ideeën aan te dragen.

In de politiecasus krijg ik na het succesvol doorlopen van een antecedentenonderzoek officieel de status van stagiaire bij het politiekorps. Bij deze status hoort een toegangspas voor de beleidsafdeling van mijn twee sleutelinformanten en voor de ANPR-divisie. Ook krijg ik een e-mail account, gebruikersnaam en wachtwoord voor het computernetwerk en fysieke werkplek. Ik kan naar believen binnen komen lopen. Het politiekorps verleent mij deze toegang, omdat het geïnteresseerd is in legitimiteitsvraagstukken betreffende ANPR. Ik beloof om aandacht te besteden aan de vragen die zij hebben en een adviesrapport te schrijven. Mogelijk zorgt mijn aanwezigheid ervoor dat informanten zich iets zelfbewuster gedragen dan ze anders zouden doen. Om te voorkomen dat zij het gevoel krijgen dat ze zichzelf te veel blootgeven of misschien in een lastige positie manoeuvreren en om hen te stimuleren om vrijuit te spreken en te handelen beloof ik vanaf het begin anonimiteit aan zowel individuele actoren als het politiekorps als geheel.

In de NDW-casus krijg ik niet zo’n formele status als in de politiecasus, maar zorgt mijn aanwezigheid er vanzelf voor dat ik geleidelijk aan onderdeel wordt van het projectteam. Voor de beleidsactoren wordt het ‘gewoon’ dat ik erbij ben. Tijdens koffiepauzes praat ik gewoon mee over (privé)onderwerpen die niets met de aanbesteding te maken hebben. Ik laat bewust na om mijn mening te geven over de

inhoud van de overleggen om de lopende discussie niet al te zeer te beïnvloeden. Ik lever geen verbale bijdrage, maar ik kan niet uitsluiten dat ik non-verbale tekens afgeef. Zo heb ik wel eens oogcontact met één van mijn sleutelinformanten, waarbij ik een glimlach of enig rollen met de ogen niet kan inhouden. Naarmate het aanbestedingstraject vordert, kost het mij steeds meer moeite om me afzijdig te houden van de inhoud, omdat ik me daadwerkelijk deelgenoot begin te voelen van wat de projectgroep probeert te bereiken. Ik voel blijdschap als er voortgang is en ben wel eens verontwaardigd als iemand in mijn visie het traject frustreert. Soms proberen de aanwezigen mij wel eens uitspraken te ontlokken over mijn kijk op de gang van zaken door dingen te zeggen als: *‘Je zal wel denken: “wat een druktemakers”.’*, *‘Waar let je nu allemaal op?’* of *‘Interessant hè, wat we allemaal bespreken?’*. Doorgaans reageer ik hierop met een glimlach en de vraag hoe zij het zelf vinden gaan. Dat beïnvloeding niet altijd te voorkomen is, wordt duidelijk tijdens een van de laatste interviews in de NDW-casus. Ik vraag de informant of er over de resultaten van het aanbestedingsproces wordt gecommuniceerd met burgers, waarop hij antwoordt: *‘Geen idee, maar dat is een goed punt. Ik schrijf het gelijk op om te bespreken wie dat moet gaan doen.’*

3 Analyse van onderzoeksgegevens

Bij de analyse van de gegevens uit de observaties, interviews en documenten zet ik voor iedere casus de volgende stappen:

a. *Identificeren van technologie- en legitimiteitsassumpties*

Uit het onderzoeksmateriaal identificeer ik de fragmenten die verwijzen naar:

- Beoogde en gerealiseerde beleidstoepassingen van technologie.

Overwegingen met betrekking tot de legitimiteit van de technologie identificeer ik door het selecteren van:

- Verwijzingen naar wetten, regels en procedures (legaliteit).
- Verwijzingen naar (ethische) waarden (normatieve rechtvaardiging).
- Verwijzingen naar opinies en gedragingen onder burgers en autoriteiten (maatschappelijke acceptatie).

De gevonden fragmenten over technologie en legitimiteit groepeer ik vervolgens per onderwerp. Zo stel ik vast welke beleidstoepassingen de politie en NDW toeschrijven aan de surveillancetechnologie. Ook de verwijzingen naar legitimiteit groepeer ik per onderwerp. Welke wetten, regels en procedures worden van belang geacht in de beleidsvorming over mobiliteitssurveillance? Welke waarden worden in het beleid

aangehaald? Op welke punten in de beleidsvorming wordt rekening gehouden met de mening van burgers en/of autoriteiten?

Het gaat hierbij om technologie- en legitimiteitsassumpties van de Politie Noodaalstad en NDW en niet van mijzelf. Zo geeft legitimiteitsassumptie 12 in de politiecasus, ‘De politie mag op grond van de Wet Politiegegevens ANPR-analyses uitvoeren ten aanzien van concrete criminaliteitsproblemen. (legaliteit)’, weer dat de Politie Noodaalstad van mening is dat ze de Wet Politiegegevens zodanig kan interpreteren dat deze haar een legitimiteitsgrond biedt om ANPR-analyses uit te voeren. Op basis van de door mij gegenereerde empirische gegevens stel ik vast dat de politie deze opvatting heeft. Vervolgens wijs ik deze toe aan de legitimiteitscategorie legaliteit, omdat deze assumptie betrekking heeft op een wet.

b. Bepalen van surveillanceperspectieven

De gevonden technologie- en legitimiteitsassumpties vergelijk ik met de technologie- en legitimiteitsassumpties die ik in hoofdstuk 4 per theoretisch surveillanceperspectief heb vastgesteld. Tabel 6 geeft deze weer. Door het verbinden van de empirisch aangetroffen technologie- en legitimiteitsassumpties aan die van de surveillanceperspectieven wordt inzichtelijk op welke punten het beleid van het politiekorps en dat van NDW kenmerken vertonen van de drie surveillanceperspectieven controle, interactie en voorzorg. Mogelijk zijn er ook technologie- of legitimiteitsassumpties die niet duidelijk toe te schrijven zijn aan één van de surveillanceperspectieven. Voor die onderwerpen raadpleeg ik nogmaals het empirisch materiaal om te begrijpen of er mogelijk sprake is van een alternatieve visie op surveillance.

CONTROLEPERSPECTIEF	
<i>Technologieassumpties</i>	<i>Legitimiteitsassumpties</i>
<u>Wijdverspreide controle van burgers</u> Surveillancetechnologie geeft de overheid de mogelijkheid om burgers wijdverspreid te controleren op afwijkend gedrag door in de rol van kijker zoveel mogelijk gegevens over zo veel mogelijk burgers als bekeken in te winnen en te verwerken.	<u>Inzet van surveillance ten aanzien van burgers</u> a) Juridische gronden voor het toestaan en/of gebieden van de inzet van surveillance zijn van belang. b) Normatieve rechtvaardiging voor de inzet van surveillance is van belang. c) Maatschappelijke acceptatie van de inzet van surveillance is van belang.
<u>Disciplineren van burgers</u> Surveillancetechnologie geeft de overheid de mogelijkheid om burgers te disciplineren door in de rol van kijker aan burgers als bekeken kenbaar te maken dat er een controlesysteem is zonder details te geven over de exacte toepassing hiervan.	<u>Beschermen van privacy van burgers</u> a) Juridische gronden voor de bescherming van de privacy van burgers zijn van belang. b) Normatieve rechtvaardiging voor de bescherming van de privacy van burgers is van belang. c) Maatschappelijke acceptatie van de bescherming van de privacy van burgers is van belang.
INTERACTIEPERSPECTIEF	
<i>Technologieassumpties</i>	<i>Legitimiteitsassumpties</i>
<u>Verbinden van overheid en burgers</u> Surveillancetechnologie kan overheid en burgers met elkaar in verbinding brengen.	<u>Toegang tot surveillance-informatie</u> a) Juridische gronden voor het verkrijgen van en/of het verplichten tot toegang tot surveillance-informatie zijn van belang. b) Normatieve rechtvaardiging voor het verkrijgen van en/of het verplichten tot toegang tot surveillance-informatie is van belang. c) Maatschappelijke acceptatie van het verkrijgen van en/of het verplichten tot toegang tot surveillance-informatie is van belang.
<u>Gezamenlijke informatiecreatie</u> Surveillancetechnologie stelt overheid en burgers in staat om informatie over zichzelf en elkaar te creëren, te beoordelen en aan te passen.	<u>Relevantie en kwaliteit van surveillance-informatie</u> a) Juridische gronden voor de beoordeling van relevantie en kwaliteit van surveillance-informatie zijn van belang. b) Normatieve rechtvaardiging voor de relevantie en kwaliteit van surveillance-informatie is van belang. c) Maatschappelijke acceptatie van de relevantie en kwaliteit van surveillance-informatie is van belang.

VOORZORGPERSPECTIEF	
<i>Technologieassumpties</i>	<i>Legitimiteitsassumpties</i>
<u>Identificeren van risico's en risicoburgers</u>	<u>Definiëring van risico's en risicocategorieën burgers</u>
Surveillancetechnologie geeft de overheid de mogelijkheid om risico's en risicoburgers te identificeren.	a) Juridische gronden voor het definiëren van risico's en risicocategorieën burgers zijn van belang.
<u>Beteugelen van risico's</u>	b) Normatieve rechtvaardiging voor het definiëren van risico's en risicocategorieën burgers is van belang.
Surveillancetechnologie geeft de overheid de mogelijkheid om risico's te beteugelen door bepaalde groepen burgers extra in de gaten te houden.	c) Maatschappelijke acceptatie van het definiëren van risico's en risicocategorieën burgers is van belang.

Tabel 6: Technologie- en legitimiteitsassumpties in het controle-, interactie- en voorzorgperspectief

c. Vaststellen implicaties voor de relatie overheid-burger

Als laatste analysestap ga ik in op wat de in het beleid aangetroffen surveillance-perspectieven betekenen voor de relatie overheid-burger. Hierbij bespreek ik op welke punten de theoretisch verwachte invulling van de verhoudingen machthebber-onderdaan, dienstverlener-cliënt en democratisch instituut-citoyen empirisch tot uiting komt. Zodoende ontstaat een empirische inkleuring van het theoretisch kader dat ik aan het eind van hoofdstuk 4 heb gepresenteerd.

In de hoofdstukken 6 en 7 vertel ik de verhalen van de twee casussen. In deze verhalen ga ik nader in op de hoofdrolspelers, de organisaties waar ze werkzaam zijn, de achtergrond en het verloop van de beleidsvorming waar ze deel van uitmaken. Aansluitend aan ieder verhaal geef ik de analyse van de onderzoeksgegevens. Vervolgens breng ik in hoofdstuk 8 de resultaten van de twee casestudy's samen om tot een antwoord op de centrale onderzoeksvraag te komen.

HOOFDSTUK 6

AUTOMATISCHE NUMMERPLAATHERKENNING IN DE POLITIEREGIO

NODAALSTAD⁴¹

‘Het gaat er om dat je eerst gaat kijken naar wat je zelf wil en niet naar wat kan. Want er kan heel veel, maar je moet je niet laten opnaaien door al dat technische gedoe. Dus we hebben daar een echte toepassingsvraag van gemaakt in ons gebied.’

(Korpsleiding)

1 Inleiding

Automatic Number Plate Recognition (ANPR) is ‘een techniek waarmee een camera met onderliggende software op straat mobiel of statisch kentekens scant en deze kentekens direct matcht met kentekens in een bestand, een hotlist’, aldus een beleidsdocument van de Politie Nodaalstad.⁴² ANPR stelt de politie in staat om mobiliteitsgegevens over burgers in te winnen, te koppelen en te analyseren en is als zodanig te beschouwen als een manifestatie van publieke mobiliteitssurveillance.⁴³ Sinds de eerste politietoepassing in Nederland, medio jaren negentig,⁴⁴ is ANPR bij de grotere politiekorpsen zoals Nodaalstad uitgegroeid tot een complex systeem dat verkeersgegevens kan vertalen naar waardevolle politie-informatie. Ten tijde van het casusonderzoek, dat plaatsvindt van september 2008 tot april 2009, neemt ANPR een prominente plaats in binnen het korpsinformatiebeleid, zowel in de dagelijkse politiepraktijk als in de strategiebepaling voor de (nabije) toekomst.

⁴¹ Resultaten van de onderhavige casestudy zijn eerder gepubliceerd in Van Ooijen (2011) en Van Ooijen en Bokhorst (2012).

⁴² De Politie Nodaalstad is een fictieve aanduiding voor één van de 26 politiekorpsen die Nederland rijk is vóór de invoering van de Nationale Politie op 1 januari 2013. De daadwerkelijke naam van het korps houd ik op verzoek van het korps zelf geheim. De aanduiding ‘Nodaalstad’ is een verzinsel van mijzelf, dat gebaseerd is op de prominente aandacht voor de politiestrategie nodale oriëntatie in het ANPR-beleid van dit korps. Deze politiestrategie licht ik verderop in dit hoofdstuk nader toe. Omwille van de anonimiteit heb ik afzonderlijke organisatieonderdelen en straten tevens een andere naam gegeven.

⁴³ ANPR staat niet exclusief ter beschikking van de politie, maar is ook in handen van andere publieke en private instanties. Voorbeelden zijn het publieke gebruik van ANPR door Rijkswaterstaat voor verkeersmanagement en het private gebruik bij de beveiliging van pompstations. In dit hoofdstuk ligt de focus op ANPR-gebruik bij de Politie Nodaalstad.

⁴⁴ Het KLPD maakt als eerste politiekorps in Nederland gebruik van ANPR-technologie. Deze eerste politietoepassing betreft voornamelijk verkeerscontroles. Zie Politie Rotterdam-Rijnmond, Korps Landelijke Politiediensten en VtS Politie Nederland (2008).

In dit hoofdstuk analyseer ik in hoeverre de surveillanc perspectieven controle, interactie en voorzorg aanwezig zijn in de beleidsontwikkeling over ANPR bij de politie Nodaalstad en welke implicaties voor de relatie overheid-burger hieraan verbonden zijn. Eerst geef ik een introductie op het Nodaalse ANPR-systeem om een indruk te geven van de technische en organisatorische middelen die het korps ter beschikking staan. Vervolgens beschrijf ik wat ANPR betekent in de beleidspraktijk en -ontwikkeling van de Politie Nodaalstad. Hierbij ga ik achtereenvolgens in op de volgende drie beleidsthema's: handhaving, opsporing en nodale oriëntatie. Deze drie thema's worden chronologisch geïntroduceerd in het Nodaalse ANPR-beleid en drukken op het moment van veldonderzoek alle drie een stempel op de beleidspraktijk en -ontwikkeling. Ik laat zien dat deze drie thema's in de loop der jaren steeds verder vervlochten raken, hetgeen de korpsleiding voor uitdagingen stelt als het gaat om de legitimiteit van het ANPR-beleid.

Bepalend voor de beleidsontwikkeling rondom ANPR zijn de veronderstellingen die de politie erop nahoudt over de functie van ANPR in het politiewerk (technologie-assumpties) en over de criteria die van belang zijn bij het bepalen van de grenzen van de toepassing van ANPR (legitimiteitsassumpties). Door de casusbeschrijving heen plaats ik tekstballonnen met door mij aangetroffen technologie- en legitimiteits-assumpties bij passages die illustratief zijn voor de betreffende assumpties.⁴⁵

In de daaropvolgende paragraaf volgt de analyse van het Nodaalse ANPR-beleid. In de analyse vat ik ten eerste samen welke technologie- en legitimiteitsassumpties uit het ANPR-beleid spreken. Als tweede stap van de analyse verbind ik de aangetroffen technologie- en legitimiteitsassumpties aan degene die ik in hoofdstuk 4 per theoretisch surveillanc perspectief heb vastgesteld. Zo wordt inzichtelijk in hoeverre de Politie Nodaalstad in het ANPR-beleid een controle-, interactie- of voorzorgsperspectief op surveillanc laat zien. Als derde en laatste analysestap ga ik in op wat de in het beleid aangetroffen surveillanc perspectieven betekenen voor de relatie overheid-burger. Hierbij bespreek ik op welke punten de theoretisch verwachte invulling van de verhoudingen machthebber-onderdaan, dienstverlener-cliënt en democratisch instituut-citoyen empirische werkelijkheid wordt. Zodoende ontstaat een empirische inkleuring van het theoretisch kader dat ik aan het eind van hoofdstuk 4 heb gepresenteerd.

⁴⁵ Het gaat hierbij om technologie- en legitimiteitsassumpties van de Politie Nodaalstad en niet van mijzelf. Zo geeft legitimiteitsassumptie 1 'Voor toegang tot ANPR-gegevens van gemeentecamera's is bestuurlijke toestemming nodig,' een opvatting van de Politie Nodaalstad weer, die ik heb vastgesteld op basis van de door mij gegenereerde empirische gegevens en vervolgens heb toegewezen aan de legitimiteitscategorie maatschappelijke acceptatie.

2 Het Nodaalse ANPR-systeem: technologie en organisatie

Het Nodaalse ANPR-systeem bestaat uit camera's met onderliggende software om gegevens mee te verzamelen, databases om de gegevens in te bewaren en te ordenen, een netwerkverbinding voor toegang tot de gegevens en software voor gegevenskoppeling en -analyse. Het korps heeft eind 2008 de beschikking over een arsenaal aan mobiele en vaste camera's dat voor uiteenlopende doeleinden wordt ingezet (zie paragraaf 3). Medio 2004 begint het ANPR-gebruik bij de politie Nodaalstad vanuit een onzeker enthousiasme over de technologie:

'Het allereerste begin was dat politiemensen van onze verkeerspolitie in Engeland waren gaan kijken, het daar gezien hebben en gedacht hebben: "Hé, dit kan voor ons ook iets betekenen". Dan gaat zich dat ontwikkelen totdat iedereen vindt dat het wel iets is, maar we nog niet weten hoe. Dan ga je heel voorzichtig een eerste apparaat aanschaffen, een tweede apparaat aanschaffen en ermee experimenteren. Heel voorzichtig kristalliseert zich dat natuurlijk uit in de loop van de tijd en dan groeit dat in zo'n twee drie jaar naar de situatie die we dan nu gaan creëren.'

(Middenmanager)

Technologieassumptie 1:

ANPR heeft een nog nader te bepalen nut voor de politie.

Over de eerste toepassing in Nodaalstad zegt een andere politiefunctionaris in het middenmanagement:

'Het is op kleine schaal begonnen met het uittesten van de technologie an sich. Van goh, kan dat dan en werkt dat dan? De eerste camera zat op een auto. Die reed dan rond en nam kentekens op. Het werkte allemaal. Vervolgens is er een vertaalslag gemaakt om het op veel grotere schaal te gaan toepassen.'

Het opschalen van het Nodaalse ANPR-systeem gebeurt in drie projectfasen. Tijdens de eerste fase, in 2006, worden drie herkenbare surveillancevoertuigen uitgerust met ANPR. Deze worden zowel rijdend (scannen van geparkeerde auto's) als statisch (scannen van passerende voertuigen) ingezet. In de tweede fase, die van 2007 tot in 2008 doorloopt, wordt het mobiele gebruik van ANPR aangevuld met de plaatsing van vaste camera's op de drie grote toegangswegen tot de stad. Daarnaast worden in het kader van persoonsbeveiliging vaste ANPR-camera's geplaatst rondom de woning van

een hooggeplaatste publieke functionaris. Inmiddels zijn er zeven mobiele ANPR-voertuigen, waarvan zes opvallende surveillancevoertuigen en één onopvallende bus: de zogenaamde James-Bond-bus. Ook komt in de tweede fase een operationele backoffice (BOF) tot stand en is deze toegankelijk vanaf iedere politiewerkplek in de regio Nodaalstad. Eind 2008 gaat de Nodaalse ANPR de derde projectfase in, die tot maart 2009 zou moeten lopen. Volgens het projectplan is de derde fase, die tijdens het casusonderzoek van start gaat tevens de laatste, wat niet betekent dat *‘alles rondom ANPR dan is afgerond, maar datgene wat er nog ligt wordt overgedragen aan de lijn’* (Projectplan ANPR derde fase). Met de afronding van de derde fase zou ANPR dus een structurele plek in de politieorganisatie moeten krijgen.

Vóór het eind van 2009 is een forse uitbreiding in de ANPR-apparatuur gepland. Deze betreft een toevoeging van acht cameralocaties onder korpsbeheer en de aansluiting van 70 deels bestaande cameralocaties van de gemeente, die primair bedoeld zijn voor milieucontroles (15 locaties) en verkeerstellingen (55 locaties). Met de groei van het netwerk van vaste cameralocaties neemt het dekkinggebied flink toe. Over de aansluiting van de reeds aanwezige 319 gemeentelijke verkeerscamera's op 55 locaties alleen al vermeldt het projectplan:

‘Het aansluiten van deze camera's betekent dat ineens het aantal ANPR camera's vertienvoudigd wordt: Politie Nodaalstad heeft momenteel zo'n 30 ANPR camera's in gebruik. Met de berekening van de benodigde gegevensopslag is rekening gehouden met de uitbreiding.’

Dat deze uitbreiding geen toekomstmuziek is, wordt duidelijk uit de toelichting van een middenmanager:

‘De gemeente is met dezelfde technologie onderzoek gaan doen naar verkeersstromen, intensiteit en belasting van het wegennet. Dus enerzijds zijn we bezig ANPR-camera's van onszelf te bouwen om beheersing te krijgen op alle belangrijke knooppunten in de regio en tegelijkertijd zie je dat eigenlijk de hele regio onder beheer staat van ANPR-camera's. Alleen worden de gegevens van die gemeentecamera's niet door ons opgeslagen, maar inmiddels hebben we hier wel in sommige gevallen nu al toegang toe. Dus ja, wij hebben heel veel informatie die we kunnen gebruiken.’

Technologieassumptie 2:

ANPR kan zorgen voor beheersing.

Bijvoorbeeld als er een moord gepleegd is, en we hebben gedeeltes van kentekens of hele kentekens. Dan kunnen we een analyse uitvoeren om te zien of dat kenteken ergens gereden heeft, of misschien ook niet, en welke richting het is uitgegaan. Of je kan zien of hij daar vaker is geweest, en op welke tijdstippen. Ook kan je door kentekens die steeds gecombineerd in een bepaalde tijdsfase met elkaar op een bepaalde positie zijn, zien door wie hij steeds vergezeld was. Dus dat is een geval waarbij je informatie haalt uit gemeentecamera's.'

Wel is de politie er zich bewust van dat er nog wat juridische en bestuurlijke haken en ogen zitten aan het benutten van deze ANPR-gegevens, maar maakt zich hier niet al te druk om:

'De politie wil de gegevens gebruiken voor haar eigen taken, dat is een ander doel. Dat betekent dat er een bestuurlijke, een juridische/privacy-discussie gevoerd moet worden voordat de politie gebruik kan gaan maken van de cameragegevens. Ook is er bestuurlijke toestemming nodig via de gemeente (B&W) om de gegevens te kunnen gaan gebruiken, dit is een discussie die opgestart wordt door de betrokken gemeentelijke dienst. Pas als de beide discussies geslecht zijn dan kan overgegaan worden tot het leveren van de gegevens. Vooruitlopend daarop kunnen wel een deel van de technische voorbereidingen plaatsvinden.'

(Projectplan ANPR derde fase)

Legitimiteitsassumptie 1:

Voor toegang tot ANPR-gegevens van gemeentecamera's is bestuurlijke toestemming nodig. (maatschappelijke acceptatie)

De uitbreiding van het beschikbare camera-arsenaal impliceert een behoorlijke toename aan ANPR-gegevens, en daarmee potentieel bruikbare politie-informatie. Van één vaste cameralocatie, waar camera's 24 uur per dag en zeven dagen per week aanstaan, worden per dag gemiddeld ruim 80.000 voertuigpassages geregistreerd. Over bijna iedere voertuigpassage worden de gegevens (foto's, kenteken, locatie en tijd) opgeslagen in de BackOffice Facility (BOF) van het korps, een softwarepakket dat de

politie helpt om autorisaties te realiseren, analyses uit te voeren en hotlists te creëren en te managen.⁴⁶

Ten tijde van het casusonderzoek worden alle ANPR-gegevens vier maanden bewaard, en langer bij gebruik in strafrechtelijk onderzoek. Bijgevolg bevat de BOF miljoenen gegevens die het korps ter beschikking staan. De BOF wordt beheerd door de vier medewerkers van de lokale ANPR-datadivisie (LAD), een onderdeel van de dienst die onder andere verantwoordelijk is voor het informatiebeleid van de Politie Noodaalsstad. Pas in de loop van 2007 wordt ANPR organisatorisch ondergebracht bij de dienst voor informatiebeleid. Tot die tijd was de organisatie van ANPR-activiteiten in handen van de verkeerspolitie, omdat ANPR hoofdzakelijk werd toegepast in het kader van verkeershandhaving. De organisatorische verhuizing van verkeerspolitie naar informatiepolitie is te begrijpen als een poging van het korps om meer grip te krijgen op het almaar groeiend aantal toepassingsmogelijkheden van ANPR, zo bevestigt een diensthoofd:

‘Helemaal aan het begin was ANPR zo nieuw dat je er allemaal mee te maken had. Wat ga je doen? Wat is eigenlijk de bedoeling van het geheel? Heel zachtjes aan structureert zich dat wel een klein beetje. Dan krijg je dus een lijn tussen diensthoofd en hoofd. [...] Dat is ook het kenmerkende van iets waarvan je weet: het zal zijn nut gaan hebben voor ons als politie, maar hoe nou precies? Dan gaan we zoeken. Dat noemen we dan portefeuille.’

Zodoende komt er een portefeuillehouder ANPR, wordt een stuurgroep ingesteld en wordt voornoemde lokale ANPR-datadivisie (LAD) opgericht. Samen moeten zij het in het projectplan omschreven algemene doel van ANPR gaan realiseren:

‘Het algemeen doel bij de verdere toepassing van de ANPR-techniek is het veiliger maken van het publieke domein door het beperken van het gebruik van de openbare weg door criminelen casu quo het verhogen van de pakkans van criminelen/overtreders die gebruik maken van de openbare weg. Uit de Engelse voorlopers van het ANPR-project:

Technologieassumptie 3:

ANPR verhoogt de pakkans van criminelen en overtredders.

⁴⁶ Niet alle verzamelde ANPR-gegevens worden opgeslagen in de BOF. Om technische redenen is de mobiele ANPR-apparatuur, met uitzondering van de James-Bond-bus niet aangesloten op de BOF, zo hoor ik van een betrokkene bij het ANPR-projectplan.

“denying criminals the use of the roads”. Opmerking: Met criminelen/ overtredders wordt bedoeld mensen die zich niet aan de binnen de Nederlandse wetgeving gestelde regels wensen te houden.’

(Projectplan ANPR derde fase)

Concreet krijgt deze doelstelling gestalte in drie beleidsthema's. Ten eerste richt de dienst informatiebeleid zich op de uitbreiding van ANPR-activiteiten die vanaf het begin zijn ontwikkeld in het kader van verkeershandhaving. Het tweede beleidsthema is de toepassing van ANPR in de opsporing van criminelen. Dit tweede toepassingsgebied wordt eveneens vanuit het uitvoerende deel van de politieorganisatie geïnitieerd en verder ontwikkeld, maar blijkt de dienst- en korpsleiding al snel te confronteren met legitimiteitsvragen die op hun beurt van invloed zijn op het gebruik van ANPR in de opsporingspraktijk. Met het derde beleidsthema, de nodale oriëntatie, probeert de Dienst Informatie een beleidsmatige inbedding te realiseren voor de reeds gerealiseerde ANPR-activiteiten en tegelijkertijd een weg te plaveien voor activiteiten die niet onder de traditionele politietaak vallen.

3 ANPR: van verkeershandhaving tot opsporing en nodale oriëntatie

3.1 ANPR voor verkeershandhaving

Om een indruk te krijgen van de langstlopende ANPR-toepassing bij de Politie Nodaalstad ANPR, die voor verkeershandhaving, woon ik in september 2008 een zogenaamde ‘ANPR-actie’ bij. Zichtbaar trots leidt het hoofd van de lokale ANPR datadivisie (LAD), één van mijn sleutelinformanten, mij aan het begin van de middag rond over de locatie. Hij vertelt me dat hier zo’n zeven à acht keer per jaar een actie wordt gehouden. Op het terrein, gelegen aan één van de drukste verkeerswegen van de regio, maken zo’n 50 politiemensen en een handvol medewerkers van de Douane, RDW en Belastingdienst zich klaar voor een toestroom aan ‘klanten’. De douanemedewerkers bereiden zich onder andere voor op het controleren van onterecht gebruik van rode diesel,⁴⁷ de RDW is ter plaatse om voertuigen technisch te controleren en de Belastingdienst is vooral geïnteresseerd in mensen met schulden voor de motorrijtuigenbelasting. ‘Heb je het bestand?’, vraagt één van de medewerkers van de Belastingdienst aan mijn rondleider. ‘Het bestand’ duidt op de hotlist: tabellen met kentekens waar iets mee aan de hand is, zoals een belastingschuld, maar ook overtredingen en vergrijpen die de politie zelf heeft geregistreerd, van snelheids-

⁴⁷ Rode diesel is diesel of gasolie waarvoor een laag accijnstarief geldt en waar een rode kleurstof aan is toegevoegd. Voor een nadere toelichting zie Rijksoverheid (2012a).

overtredingen tot drugsrunnen. De LAD-chef zorgt ervoor dat de hotlist voor iedere actie wordt ververst en meegenomen naar de locatie.

Voordat de actie echt van start gaat, wijst mijn rondleider mij glunderend op de aanwezigheid van een filmploeg van het televisieprogramma ‘Op de bon’: *‘Je hebt geluk vandaag’*. Ik voel het enthousiasme onder de aanwezigen over wat er staat te gebeuren en ook een stilte-voor-de-storm-spanning. Ieder moment kan de actie van start gaan, die van 14.00 uur tot 22.00 uur zal duren. Plots zie ik dat de ene na de andere auto het terrein op wordt geleid om ontvangen te worden door agenten ter plaatse. Er is plek voor 15 à 20 auto’s tegelijkertijd. Eén van de agenten spreekt blijmoedig van een ‘service’ aan burgers als hij het heeft over de hotlist van mensen die in het verleden zijn aangehouden als dronken bestuurder. Hij vergelijkt deze mensen met patiënten in het ziekenhuis die ook wel eens op controle komen. Blijkbaar staat er een lijst met kentekens van dronken bestuurders in ‘het bestand’. Over het algemeen zijn de aangehouden bestuurders redelijk kalm en werken ze goed mee aan de controle. Dat dit niet voor iedereen het geval is, wordt mij duidelijk als mijn begeleider mij wijst op het ‘pad voor vuurgevaarlijken’. Aan het eind van dit pad staat een politiebusje klaar voor inhechtenisneming. Nog een aparte plek op het terrein is gereserveerd voor de inbeslagname van voertuigen, die met name plaatsvindt voor mensen met hoge belastingschulden. Later vraag ik aan een middenmanager of aangehouden bestuurders wel eens protest of bezwaar aantekenen tegen de gevoerde werkwijze van de politie.

‘Kijk je hebt ook niet zoveel te vertellen als je nog drieduizend euro aan boetes open hebt staan. Dan kan je daar wel bezwaar tegen gaan maken, maar dat schiet niet echt op. Het is gewoon zo. En je staat al in het systeem. Het is niet zo dat wij een nieuw systeem aanleggen. Je staat al in het systeem. Alleen kunnen we je op basis van het systeem er uithalen. Dus geregistreerd sta je al. Je staat al in een databestand. En je auto ook al. Het enige punt is dat je deze bestanden naast elkaar legt en dus heel snel geautomatiseerd kijkt wie er langs rijdt. Want meer is het niet.’

Legitimiteitsassumptie 2:

De politie mag ANPR gebruiken, omdat het de uitvoering van de politietaak betreft. (legaliteit)

‘Als ze allemaal langzaam zouden rijden en het zouden maar vijf kentekens zijn, dan zou ik het met mijn zakboekje ook kunnen. Dan zou ik ze er ook uithalen. Nou aangezien het er duizenden zijn en honderdduizenden die langsrijden, kan ik dat niet. Daarom doen we het geautomatiseerd met die systematiek en die techniek. En ja, dan halen we je eruit. Ik heb nog niet meegemaakt dat er eentje zei: “Nou, dit is onrechtmatig dat u mij...”. Nee. Dat gaat ook niet gebeuren. Er is natuurlijk altijd wel een of andere advocaat die denkt dat hij het ei van Columbus heeft uitgevonden. Maar over het algemeen wordt er geen bezwaar gemaakt tegen de methodiek. Het heeft ook al honderd keer in de krant gestaan, dat die camera’s daar hangen. En nog rijden al die mensen hierlangs, ook al degenen die boetes open hebben staan, en die geen rijbewijs hebben en die vaak alcohol drinken. Ja.’

Legitimitéitsassumptie 3:

ANPR is legitiem op grond van kenbaarheid van enkele kenmerken van het systeem. (maatschappelijke acceptatie)

Dan word ik per auto meegenomen naar de zogenaamde ‘James-Bond-bus’, die enkele honderden meters van het controleterrein staat. Vanuit dit op het eerste gezicht onopvallende busje worden de escortes naar het terrein in gang gezet. De twee ANPR-camera’s die op deze bus zijn gemonteerd maken gedurende de actie, die ongeveer acht uur in beslag neemt, foto’s van alle voertuigen die langs rijden. Op het moment dat de schuifdeur van de bus wordt opengetrokken, kan ik zien hoe het proces dan verdergaat. In de bus kijkt een agent geconcentreerd naar een groot beeldscherm en geeft intussen instructies via de portofoon. Ik maak mee dat er een aantal malen een hit op het scherm verschijnt. Dit betekent dat er op dat moment een auto langsrijdt waarvan de kentekenplaat één of meerdere keren voorkomt in een hotlist. Op het beeldscherm zie ik verschillende gegevens over het gescande voertuig verschijnen. Zo zijn daar een zwart-witfoto van de kentekenplaat met contouren van het voertuig en de van de foto afgeleide kentekengegevens in cijfers en letters. Bij sommige hits levert de database ook informatie over het merk, type en kleur van de auto, maar dat is niet standaard het geval. Verder zie ik de datum en tijd van registratie, maar blijft het veld voor GPS-coördinaten bij deze actie leeg. Later ontdek ik dat locatiegegevens wel een grote rol spelen bij ANPR-toepassingen in het kader van opsporing en nodale oriëntatie. Daarnaast toont het scherm een cijfer voor het aantal databases waar het gescande een hit voor oplevert. Ook is er een aanduiding van de betreffende databases, bijvoorbeeld

‘Rijksbelastingen’ en ‘DJI’.⁴⁸ Als laatste onderdeel is er een omschrijving van één of meerdere overtredingen of delicten waar het kenteken aan is gekoppeld, bijvoorbeeld ‘verlopen rijbewijs’, ‘verlopen APK’ en ‘drugrunner’.

De James-Bond-agent seint meteen via de portofoon de coördinatoren van de actie in, die zich bevinden in het commandovoertuig, een soort stacaravan op het controleterrein. Kenteken, merk, type en kleur worden doorgegeven, samen met de doelgroep, bijvoorbeeld ‘voor Douane’. Als er plek is op het controleterrein wordt de betreffende auto door één van de beschikbare motoragenten daar naartoe begeleid of voor het terrein aangehouden door een agent die al ter plaatse is. Bij de ingang van het terrein krijgt de auto één of meerdere gekleurde kaartjes achter de voorruit geplakt, afhankelijk van de relevante instantie: blauw voor de politie, rood voor de Belastingdienst en geel voor de Douane. Vervolgens voeren agenten een standaardcontrole uit, waaronder een rijbewijscheck. Door de verschillende aanwezige instanties is afgesproken dat de politie altijd ‘als eerste mag innen’ als er sprake is van een hit voor meerdere partijen. Zo komt het voor dat iemand eerst zijn boetes bij de politie betaalt en vervolgens wordt doorgestuurd naar de post van de Belastingdienst om daar af te rekenen. Tijdens de eerste opvang door agenten op het controleterrein geven zij via de portofoon twee andere agenten in een nabijgelegen wijkbureau instructies om de betreffende persoon na te trekken in politiedatabases die van te voren niet opgenomen waren in de ANPR-hotlist. Voor een deel is deze extra controle hetzelfde voor alle aangehouden personen, bijvoorbeeld voor openstaande overtredingen. Voor een ander deel is deze per persoon verschillend. Iemand met een verlopen rijbewijs wordt bijvoorbeeld gecontroleerd op een mogelijke rijontzegging. ANPR werkt zodoende als een tweetrapsraket: iemand wordt op basis van één of meerdere ANPR-hits uit de verkeersstroom gehaald en vervolgens aanvullend afgerekend op andere overtredingen. Het afrekenen neemt verschillende vormen aan: betalen met de pinpas, inbeslagname van de auto en/of inhechtenisneming. De politiecapaciteit is niet voldoende om alle hits daadwerkelijk af te handelen. Zo staat de volgende dag op het Nodaalse intranet vermeld: ‘Er passeerden 8476 voertuigen de scanauto, waarvan 432 “hits”. Hiervan werden 176 auto’s daadwerkelijk staande gehouden’.

Het onzekere enthousiasme uit de experimentele beginfase van ANPR heeft na een aantal jaren van toepassing in de verkeershandhaving een duidelijker fundament gekregen. *‘Er is veel enthousiasme, omdat we zien dat we resultaten boeken’*, aldus een middenmanager. Verschillende collega-leidinggevenden benadrukken naast de

⁴⁸ Dienst Justitiële Inrichtingen.

effectiviteit van ANPR de behaalde efficiencywinst. Zo hoor ik van twee functionarissen binnen de dienstleiding:

‘Je biedt jezelf de kans om iets merkwaardigs te vinden...in het gewone politiewerk. Ja, die technische middelen die gaan ons steeds meer die kans geven. Vroeger stond je op Nodaalplein en dan gaf je iedere auto een stopteken. En nu alleen degenen die op voorhand al niet goed zijn. Dat is wel efficiënt. Dat is denk ik ook iets wat je hiermee zal zien: dat je het aantal van die controles gaat beperken tot dingen die je een beetje merkwaardig vindt.’

‘Er is een bestand van mensen wier rijbewijs is ingenomen. Dat zetten we achter een camera. Dan hoeven wij dus niet te zeggen: het hele verkeer door die hoofdweg zetten wij helemaal vast, want we gaan al die auto’s controleren. Nee, we zeggen: “ploep, maatwerk; die auto, met die tenaamstelling, die eigenaar is zijn rijbewijs afgenomen.” [...] Die toepassing en die bevoegdheid heb je, had je en zal je altijd houden.’

Legitimiteitsassumptie 4:

Het is goed dat de politie ANPR inzet, omdat ze hierdoor efficiënter werkt met minder overlast voor onschuldige/onverdachte burgers.
(normatieve rechtvaardiging)

Over het nut en de legitimiteit van de toepassing van ANPR in de verkeershandhaving lijkt nauwelijks tot geen discussie te bestaan binnen het korps. Wel geeft de dienstleiding aan dat er grenzen zijn aan de aard van de hotlists die de politie wil gebruiken:

‘Met het middel ANPR selecteren wij bijvoorbeeld mensen uit die een boete van de rechter opgelegd hebben gekregen, maar nooit betaald hebben. Of die nog gevangenisstraf hebben openstaan. Met dezelfde systematiek kun je natuurlijk ook mensen eruit halen die hun hondenbelasting nog niet hebben betaald. Weegt dat nou net zo zwaar? Mag je daar dan dezelfde inbreuk op maken? Nou, ik denk niet dat dat allemaal hetzelfde weegt.’

Legitimiteitsassumptie 5:

Er zijn grenzen aan de categorieën burgers waar de politie de privacy van mag schenden met ANPR.
(normatieve rechtvaardiging)

Naar mijn idee zit daar wel een verschil tussen. En zo doen we het ook. Wat heel veel mensen bijvoorbeeld graag zouden willen doen in de ANPR-controle, is het najagen van private belangen. Denk bijvoorbeeld aan deurwaarders die achterstallige alimentatie of andere schulden willen innen. Ja, daar leggen wij ook de grens. Wij doen geen private zaken.'

Waar meer discussie over bestaat, is over het gebruik van de passagegegevens die door alle vaste camera's en de James-Bondbus worden verzameld. Voor verkeershandhaving zijn deze gegevens niet nodig, omdat de opvolging van een hit onmiddellijk volgt op de voertuigpassage. Dat een voertuig met een hit op bijvoorbeeld openstaande boetes op tijdstip t locatie l passeert, wordt irrelevant voor de verkeershandhaving op het moment dat dit voertuig op tijdstip t en locatie l wordt staande gehouden om de betreffende hit af te handelen. Om andere redenen heeft de politie echter wel belang bij het bewaren van passagegegevens. Eén van die redenen is het opsporingsbelang, dat ik in de volgende subparagraaf bespreek.

3.2 ANPR voor opsporing

3.2.1 Scannen en signaleren in de omgeving

De politiefunctionarissen in het veld benutten de extra apparatuur die tussen 2004 en 2007 tot hun beschikking komt niet alleen voor een schaalvergroting in de verkeershandhaving, maar starten ook initiatieven om ANPR in te zetten bij opsporingsonderzoek. *'De toepassing van ANPR in de criminaliteitsbestrijding kwam op gang toen men bij een zwaar delict dacht "laten we ANPR gebruiken om de omgeving te scannen."'*, aldus het management van de Dienst Informatie. Een manager van een Team Grootschalig Opsporingsonderzoek (TGO) vertelt hoe het begon:

'Ik denk dat wij er in 2007 echt mee aan de gang zijn gegaan, en in 2008 hebben we er ook echt het rendement van gezien. [...] In de eerste fase was het van: "ok, als dit ook binnen handhaving wordt toegepast, welke kansen geeft het dan binnen de opsporing?" Die discussie hebben we toen gekregen. Vanuit die situatie zijn we het ook feitelijk gaan gebruiken. Hierbij maken we niet alleen gebruik van de wetenschap dat er ergens een ANPR-camera is geplaatst, maar zetten ook op bepaalde plaatsen een mobiele ANPR in, omdat er bijvoorbeeld een belangrijke ontmoeting plaatsvindt waarbij je een aantal kopstukken geregistreerd wil hebben. Ook is het voor ons een gemakkelijk middel om bijvoorbeeld in de omgeving te laten rijden waar begrafenis-

en crematies plaatsvinden om te weten welke groep mensen ter plaatse komt. En zo gaan we het steeds creatiever gebruiken.'

Mobiele ANPR fungeert ook als een hulpmiddel bij het doen van buurtonderzoek. Een dienstmanager licht toe dat de inzet van ANPR niet betekent dat aanwezigheid op de locatie van een misdrijf sneller tot verdenking leidt.

'Als er een misdrijf is gepleegd dan worden alle kentekens in die buurt opgenomen. Maar als daar geen relatie is met het misdrijf, dan komt het echt niet in jouw dossier. Trouwens, je wordt niet eens bewaard, laat ik het zo zeggen. Er komt echt geen aantekening "stond op honderd meter van de roofmoord van de bakker". Dat is echt een illusie. [...] Als ik nu een buurtonderzoek doe, dan stel ik je ook vragen en schrijf ik je naam ook op. En dan schrijf ik toch ook niet: "Je zit nu in mijn systeem, want toen was je toevallig daar". Nee. Als je geen feitelijke relatie hebt met een incident of een misdrijf, dan word je gewoon eruit gehaald. Tenminste, ik weet eigenlijk helemaal niet eens wat er mee gedaan wordt. Het wordt niet geregistreerd of iets.'

Daarnaast worden voor de opsporing relevante hotlists geladen op de mobiele ANPR-apparatuur, zodat er direct tot aanhouding kan worden overgegaan op het moment van een hit. Deze toepassing is wezenlijk niet veel anders dan wat er gebeurt bij een ANPR-actie met het duidelijke verschil dat er geen bataljon agenten klaar staat om de hit op te volgen:

'Op dit moment kunnen we nog niet reageren op alle informatie. We moeten prioriteiten stellen. We willen dan voorrang geven aan zware delicten in de directe opvolging op vaste camera's. Bijvoorbeeld gaat het dan om de aanhouding van veroordeelde criminelen. Nu worden alleen maar mobiele camera's gebruikt voor directe opvolging van hotlists.'

(Middenmanager)

In het uitvoeringsprotocol ANPR staan vermiste personen, gestolen auto's en veroordeelden genoemd als voorbeelden van hotlists voor directe opvolging in de opsporing. Op het moment dat de directe opvolging ook wordt geactiveerd op de vaste ANPR-camera's, ontstaat er een stil alarmsysteem dat criminelen misschien niet buiten de deur houdt, maar de kans op een onopgemerkte entree danig verkleint:

‘Wanneer je weet dat een bepaald vals kenteken gebruikt wordt door potentiële terroristen of verdachte personen, dan kun je dat eruit halen. Je kunt ook een signaal krijgen op het moment dat het gedetecteerd wordt. Dus op het moment dat hij de regio inrijdt, kan je het systeem een signaal laten afgeven: dat kenteken komt nu daar en daar binnen in onze regio.’

(Dienstleiding)

Technologieassumptie 4:

Door ANPR kunnen criminelen niet ongezien de regiogrenzen overschrijden (ring of steel).

Naast de meer structurele hotlists voor directe opvolging in de opsporing, wordt er gebruik gemaakt van ‘acute hotlists’. Dit is een lijst met alle kentekens die aan een ernstig strafrechtelijk incident zijn gerelateerd. Het gaat dan bijvoorbeeld om overvallen, ontvoeringen en terrorismedreiging.

3.2.2 Bevragen en analyseren van opgeslagen ANPR-gegevens

De toepassingen van ANPR voor de opsporing blijken niet alleen te liggen in het mobiel inwinnen van gegevens, maar ook in het gebruik van reeds ingewonnen gegevens die zijn opgeslagen in de BOF. *‘De verzamelde data van gescande kentekens en bijbehorende foto’s (hits en no-hits = de “captures”) kunnen later ook worden geanalyseerd en veredeld’*, zo lees ik in het projectplan ANPR derde fase. Hoeveel ANPR-gegevens de politie ter beschikking staan, hangt niet alleen af van het aantal locaties waarop gegevens worden ingewonnen, maar ook van de tijdsperiode waarover gegevens worden bewaard: de bewaartermijn. Op het moment van het veldonderzoek worden alle gegevens, zowel de hits als de no-hits vier maanden bewaard en naderhand niet alleen in de virtuele prullenbak geleegd, maar daadwerkelijk vernietigd, met uitzondering van de gegevens die in de tussentijd zijn geselecteerd voor opsporingsdoeleinden. Eerder dat jaar is binnen de dienst informatie op basis van de nieuwe Wet Politiegegevens (Wpolg) besloten tot een bewaartermijn van één jaar, maar na *‘een verscherpte discussie met de korpsleiding’* is de portefeuillehouder ANPR genoodzaakt om de viermaandetermijn te hanteren zoals eerder was voorgeschreven in het privacyreglement ANPR uit 2007. De korpsleiding licht de discussie als volgt toe:

‘Ik had in mijn korps een discussie: we hadden 5 miljoen kentekens in het bestand staan en dat was wel lekker, want dan kon je als rechercheur nog eens een keer kijken. Die gegevens waren over de viermaandentermijn heen. Dus ik zei: “die gaan nu vernietigd worden”. Even had ik de indruk dat er iemand was die dat niet zo vond. En op het moment dat ik dat in de gaten had, heb ik gezegd: “de eerste die ik nu tegenkom, gaat onmiddellijk met ontslag”. Daar twijfel ik geen seconde over dat je daar keihard op moet zitten. Want wij zijn een betrouwbare organisatie; wij zijn de vrienden van de wet.’

Legitimiteitsassumptie 6:

De politie heeft een juridische grondslag nodig voor het bewaren van ANPR-gegevens.
(legaliteit)

In de praktijk blijkt het vernietigen van gegevens geen simpele opgave te zijn, zo vertelt de dienstleiding die de orders van de korpsleiding moet laten uitvoeren:

‘Er was afgesproken dat de opgeslagen gegevens vernietigd zouden worden. Ja, ok, en dat gaat niet helemaal naar wens. [...] Ik moet dus zorgen dat het gewoon allemaal gebeurt, dat de belemmeringen worden weggewerkt en dat het gewoon geregeld wordt. [...] Ik bemoei me dus met het onderwerp “vernietigen van gegevens” in opdracht van de korpschef en dat kan dan geen uitstel gedogen. Mensen hebben het beeld dat je in het bestand alles één keer selecteert, op een knopje drukt en dat het dan allemaal weg is. Dat is niet zo. Het kost een hoop energie om het verantwoord op te ruimen.’

De LAD-chef zorgt er uiteindelijk voor dat de gegevens worden verwijderd en vernietigd, maar is nog steeds van mening: *‘één jaar is nodig; vier maanden is te kort’*, wat ik ook terughoor van een andere operationeel leidinggevende. Evenwel verwerkt de LAD-chef eind 2008 de hernieuwd afgesproken bewaartermijn in het uitvoeringsprotocol ANPR, dat voorts vermeldt:

Legitimiteitsassumptie 7:

Het bewaren van ANPR-gegevens is nodig voor de moderne criminaliteitsbestrijding.
(normatieve rechtvaardiging)

‘De gescande kentekens worden bewaard in het ANPR-bestand. In afwachting van de te ontwikkelen beleidsvisie en verdere landelijke ontwikkeling wordt voorlopig de bewaartermijn van 4 maanden uit het Privacyreglement ANPR van 2007 aangehouden.’

Voorlopig heeft de Politie Noodaalstad de beschikking over historische ANPR-gegevens tot vier maanden terug in de tijd. Het uitvoeringsprotocol geeft aan dat er twee vormen van bevraging mogelijk zijn als het gaat om opsporing:

‘Enkelvoudige bevraging in het kader van opsporingsonderzoeken naar strafbare feiten waarop voorlopige hechtenis staat is toegestaan; het verwerken van de data ten behoeve van de vervaardiging van analyses ter ondersteuning van opsporingsonderzoeken naar strafbare feiten waarop voorlopige hechtenis staat is toegestaan.’

Enkelvoudige bevraging betreft het opvragen van ANPR-gegevens van een bepaalde kentekenplaat. Zodoende kunnen over de afgelopen vier maanden de vervoersbewegingen van een bepaald voertuig worden gereconstrueerd. De medewerkers van de LAD, die allen volledige toegang hebben tot de BOF, geven mij een demonstratie van deze functionaliteit. Bij één van hen mag ik even aanschuiven om op het computerscherm te zien hoe de BOF eruit ziet. ‘*Rij je zelf wel eens langs cameralocatie 1? Dan kunnen we je opzoeken.*’

Technologieassumptie 5:

Met ANPR kan de politie de bewegingen van een geselecteerd voertuig reconstrueren.

Ik antwoord ontkennend. Vervolgens typt de politiemedewerker zijn eigen kenteken in en er verschijnt een tabel met passages langs *cameralocatie 1*, inclusief een aantal captures van de dag van de ANPR-actie. Ik reed toen met de politieman mee en zie terug hoe we vroeg in de middag op weg naar het controleterrein langs één van de noordwaartse camera's komen. Het systeem laat zien dat we een paar uur later een zuidwaartse beweging maken richting James-Bondbus en toont nogmaals een zuid-noordpassage kort daarna. Van een bepaald kenteken is dus gemakkelijk in de BOF terug te zien of en wanneer dit langs bepaalde cameralocaties is gekomen.

Regelmatig is het aan het begin van een opsporingsonderzoek nog niet duidelijk welke kentekens hiervoor relevant zijn. Het ANPR-systeem kan dan juist gebruikt worden om die informatie te achterhalen. Er is op voorhand geen koppeling tussen kentekenplaat en delict. Analyse van passagegegevens gekoppeld aan andere gegevens in het opsporingsonderzoek moeten hier duidelijkheid in brengen. Bij dit type analyse wordt

in de loop der tijd na een (aantal) passage(s) duidelijk hoe een hit precies gedefinieerd moet worden. Dan pas is er inzicht in welke kentekenplaten horen bij bijvoorbeeld verdachten, betrokkenen of getuigen. Wederom laat ik een opsporingsmanager aan het woord:

*‘Er vindt een liquidatie plaats. Naar aanleiding van zendmastgegevens kunnen we zien dat er een viertal telefoonnummers een heel belangrijke rol hebben gespeeld ten tijde van het plegen van het feit. Dan kan je ook bepalen hoe de reisbewegingen zijn en die ga je omzetten naar onder andere je mogelijkheden met de ANPR-camera’s van de gemeente, maar zeker ook met de eigen ANPR. En waarom? Omdat als ik zie dat hij om 1 uur aanstraalt bij de zendmast van ***, en dat hij om 1 minuut over 1 aanstraalt bij de zendmast van ***, dan kan ik er eigenlijk wel van op aan dat hij door *** gereden is. Dus wat ga ik dan doen? Dan ga ik in ieder geval naar aanleiding van mijn ANPR-kansen, de beelden van één minuut tot twee minuten over één vastleggen. Die wil ik graag zien, die wil ik hebben. En dat hebben wij op een aantal vaste momenten gedaan, naar aanleiding van de historische gegevens die ik ter beschikking had. En dan kom je tot de conclusie dat er eigenlijk maar één auto geweest kan zijn en dat is de auto die elke keer zichtbaar was op die plekken. [...] Dan krijg je dus een kenteken ter beschikking en vanuit dat kenteken ga je verder rechercheren. Dan betreft het een huurauto, en vanuit die huurautovaststelling konden wij naar aanleiding van de gegevens die daar verstrekt waren én het telefoonnummer dat bij de verhuur was opgegeven, tot een koppeling van persoon komen als gebruiker van een bepaalde telefoon, huurder van een auto, in beeld bij ANPR, en ter plaatse naar aanleiding van dat telefoonnummer op het plaats delict.*

Naar aanleiding van die situatie hebben wij al die contacten in beeld gebracht en hebben we het zelfs zo ver kunnen schoppen dat we niet alleen die ene auto op die manier hebben uitgewerkt, maar ook elke keer de auto die ervoor reed en de auto die erachter reed. En zo kwamen wij tot een situatie dat we in totaliteit drie auto’s hebben kunnen koppelen aan een groep van mensen die in Nodaalstad Zuid gebruik maakten van een zogenaamd safehouse, om vanuit die plaats een moord te gaan plegen op iemand die in Nodaalstad West woonachtig was. [...]

Technologieassumptie 6:

ANPR kan helpen om verdachte voertuigen te identificeren in vervoersstromen.

Als ik geen ANPR had gehad, en dus ook niet wist over welk kenteken ik sprak, dan had ik dus ook geen vervolgvragen bij het bedrijf achter de gemeentelijke ANPR-camera's kunnen gaan stellen, want dat doen ze op kenteken. Dan had ik ook niet de beschikking gehad over de andere auto's die ik op die manier had kunnen koppelen. Dus je moet in wezen een aantal gegevens dat je vanaf het eerste moment veiligstelt, met elkaar in verband gaan brengen. En dan kan ANPR voor ons van heel groot belang zijn in de opsporing.'

Omdat voor opsporing doorgaans nog niet gelijk duidelijk is welke voertuigpassages mogelijk relevant zijn voor een bepaald onderzoek, worden in eerste instantie zoveel mogelijk gegevens rondom een bepaald delict zeker gesteld. Dit om te voorkomen dat de recherche later misgrijpt, omdat gegevens dan al vernietigd zijn conform de afgesproken bewaartermijn van vier maanden. Inmiddels hoort het opvragen van ANPR-gegevens net als telecomgegevens tegenwoordig bij de standaardprocedure van een opsporingsonderzoek.

'ANPR is inmiddels zodanig ingeburgerd in de informatievergaring van de politie, zeker in projectmatige onderzoeken, dat ANPR altijd bevraagd wordt. Als ik het persoonsdossier van een verdachte laat opbouwen, dan krijg ik daarbij bijvoorbeeld altijd kentekens die op zijn adres vermeld staan. Die kentekens worden altijd in ANPR bevraagd. Ik krijg altijd over een x periode een terugkoppeling met de tijden waarop hij gebruik heeft gemaakt van Noord-Zuid, of Zuid-Noord, of weet ik veel wat. Die krijg ik er altijd bij. Dat is een structurele situatie geworden. Als iemand nu een persoonsdossier inlevert van een potentiële verdachte en er is geen ANPR bevraagd, dan krijgt hij dat terug om dat alsnog te doen. Het is echt structureel. En zo is het in wezen als één van de opsporingsmogelijkheden binnen de opsporing geïntroduceerd. [...] Het wordt steeds moeilijker om zaken voor de opsporing van strafbare feiten daadwerkelijk te achterhalen, iemand wordt steeds handiger. [...] Tegenwoordig zijn ze bijvoorbeeld via Skype aan het telefoneren, waar politie en justitie in zijn totaliteit geen grip op hebben.

Legitimiteitsassumptie 8:

De politie is genoodzaakt ANPR te gebruiken om de politietaak nog te kunnen uitvoeren in de veranderde samenleving. (normatieve rechtvaardiging)

Dus dat houdt in dat je op een andere manier handiger moet worden. Nou één van de nog vrij simpele zaken is het toepassen van ANPR: weten waar iemand heeft gezeten, dan wel een voertuig heeft gezeten, enzovoort. En het combineren van gegevens, want dat is het allerbelangrijkste.'

(Middenmanager)

Misdaadanalisten van een opsporingsteam hebben zelf toegang tot de BOF om analyses uit te voeren en krijgen hierbij steeds meer mogelijkheden:

'De BOF kent een aantal beperkte rapportagemogelijkheden. Om de misdaadanalisten uitgebreider onderzoek te kunnen laten doen wordt er een bevragingstool gerealiseerd. [...] De nieuwe bevragingstool ANPR wordt voorzien van een GIS-faciliteit waarmee het mogelijk wordt captures en hits op een plattegrond te tonen. De bevragingstool is bedoeld voor de misdaadanalisten, [...], ze kunnen daarmee zelf hun rapportages definiëren. Complexere bevragingen, zoals een konvooi-analyse, kunnen in het bevragingstool gedaan worden. De bevragingstool kan vragen aan op willekeurige combinaties van kentekens, scans, hits, camera's en tijdstippen of periodes. Deze levert alleen niet de foto's van de captures. [...] De vragen die gebruikers gaan stellen aan het systeem zijn nog niet bekend. Ook de intensiteit waarmee het systeem gebruikt zal worden is nog onbekend. Informatie hierover zal naar voren komen in de pilot die we uit gaan voeren. Na afloop van de pilot wordt het systeem overgedragen aan de lijn.'

(Projectplan ANPR derde fase)

Niet alleen in de misdaadanalyse, maar ook in de rechtszaal wordt GIS benut voor het visualiseren van ANPR-gegevens. Zo gebruikt de Politie Nodaalstad het ANPR-systeem om dankzij no-hitgegevens retrospectief de bewegingen van een verdachte in een moordzaak te traceren en te verbinden aan de plaats delict. De manager van het betreffende opsporingsonderzoek legt uit hoe ANPR in deze zaak wordt gebruikt:

'We hebben toen een presentatie gehouden voor de rechtbank, waarin we een virtuele kaart lieten zien. Hierop werkten we met lichtjes, naar aanleiding van de waarnemingen van de historische gegevens: ANPR en camerabeelden. Op die manier konden we de verdachte als het ware zo richting plaats delict laten rijden. Dat heeft een goede impact gehad binnen de rechtszaal. Dat is natuurlijk het mooie. [...] Dat is de kracht van het combineren van je gegevens.'

Binnen de opsporing is men zich echter ook bewust van de beperkingen van ANPR. Opsporing is immers gericht op het aanhouden van personen en niet de voertuigen waar deze personen mogelijk in rijden:

‘Het nadeel aan ANPR is dat je wel goed moet weten wat ANPR weergeeft. En voor de rest moet je daar geen conclusies uit trekken. ANPR geeft gewoon weer dat een voertuig met dat kentekenplaatje daar geweest is op dat tijdstip en that’s it. Heel veel mensen maken de denkfout, dat zij weten dat jij gebruik maakt van een bepaalde auto met een bepaald kenteken, dat jij dus op die plek hebt gereden. Maar dat is niet aan de orde en daar moet je heel erg rekening mee houden. Als je zaken wilt combineren, dat jij dus gekoppeld bent aan die auto, of gekoppeld moet worden aan die auto, dan moet je dat dus op een andere manier doen dan met ANPR. Dat vind ik het nadeel ook van ANPR, wij opsporingsmensen hadden liever een veel duidelijkere foto gehad. [...] Negen van de tien keer is natuurlijk de beeldopname heel slecht, want deze is maar gericht op het kentekenplaatje en voor de rest niks. [...] Af en toe als je geluk hebt, als hij van een bepaalde kant is genomen, zie je een beetje een schim, en dat soort werk. [...] Wij zijn altijd een stuk nieuwsgieriger: wij willen ook altijd graag weten wie de bestuurder is en dat we die kunnen herkennen. Dat zou voor ons nog vele malen mooier zijn. Nou daar is men natuurlijk over in overleg om eventueel de kwaliteit, het resultaat, nog optimaler te kunnen maken. De doelstelling van ANPR is natuurlijk het kentekenplaatje lezen. Zo moet je het zien, maar daar zijn wij niet echt tevreden mee: wij willen meer. [...] Dat is geen nadeel van ANPR, maar je moet wel weten hoe je de gegevens vanuit ANPR interpreteert in je onderzoek. Dat is wel van belang. Daar moet je altijd voor waken.’

(Middenmanager)

In de beleidsontwikkeling over ANPR geeft de Dienst Informatie geen prioriteit aan de wensen vanuit het opsporingsproces. Wel is er aandacht voor de juridische toelaatbaarheid van ANPR in de opsporing door het vaststellen van de bewaartermijn en het volgen van rechtszaken elders in het land waarin ANPR een rol heeft gespeeld. Zo wijzen verschillende leidinggevendenden mij op een uitspraak van de strafraadkamer van de rechtbank Zwolle-Lelystad:

‘In de zaak die mijn collega noemt is tijdens de terechtzitting het gebruik van ANPR besproken. Ook in het proces-verbaal staat een hit op ANPR vermeld als de reden tot staande houden. In de uitspraak wordt hier echter niet op terug gekomen. Ik heb het PV en de uitspraak hier liggen. Ook is er een uitspraak bij een bevel tot gevangenhouding waarop de advocaat van de verdachte zich beroept op onrechtmatig verkregen bewijs. Dit werd echter door de rechter niet overgenomen.’

(Middenmanager)

Legitimiteitsassumptie 9:

De politie mag ANPR gebruiken in de opsporing op grond van jurisprudentie. (legaliteit)

Ook in de Nodaalse context zijn er vooralsnog geen problemen ten aanzien van de juridische acceptatie van ANPR, zo merkt een rechercheur op:

‘Ik heb tot op heden nog geen enkele vraag gehad over de acceptatie. We hebben gewoon via het proces-verbaal onderbouwd hoe we aan de data gekomen zijn en deze uitleg is gewoon aangenomen. Er kwamen geen vragen, in het geheel niet.’

De Politie Nodaalstad is vooral trots op haar ANPR-ontwikkeling. De dienstleiding zegt dan ook weinig terughoudend:

‘Kijk, ANPR bestaat al wat langere tijd, zeker in Engeland maar ook een beetje in Nederland. Maar het meest volgroeid, het meest volwassen is het korps Nodaalstad daar dan wel in. Omdat we niet alleen maar de camera’s functioneel op veel plaatsen hebben weggezet, maar ook de BOF samen met de Engelsen hebben ontwikkeld: de backoffice één maar ook vooral twee, met de analysemogelijkheden. Het hele technische en operationele gedeelte in al zijn vormen, dat is ook landelijk gewoon overgenomen.’

Parallel aan het vaststellen van de bewaartermijn en het monitoren van de acceptatie van ANPR in de rechtszaal wordt beleid ontwikkeld om ANPR-gegevens te benutten op een manier die de bestaande opsporings- en handhavingspraktijken aanvult. Nodale oriëntatie is hierbij het sleutelbegrip.

3.3 ANPR voor nodale oriëntatie

3.3.1 ANPR in een nieuw jasje

‘ANPR is nodale oriëntatie’, zo hoor ik van verschillende mensen op de eerste dag dat ik voet zet in het gebouw van de Dienst Informatie. Enkele jaren eerder, in 2005, wordt nodale oriëntatie als nieuw strategisch concept binnen het Nederlandse politiebestedel geïntroduceerd. Dit gebeurt in het rapport ‘Politie in ontwikkeling’ waarin de Raad van Hoofdcommissarissen (RvH) een heroriëntatie laat zien op de taak en positie van de politie:

‘Zowel bij burgers als binnen de kringen van gezagsdragers, bestuurders, politiek en partners in veiligheid, lopen de verwachtingen en visies over het gewenste functioneren van de politie steeds vaker uiteen. Het beeld dat de samenleving heeft van de politie wordt diffuser: waar dient de politie wel voor te staan en waar niet voor? Tegelijkertijd heerst het gevoel dat de politie beter zou moeten presteren. Waar verwachtingen en prestaties moeilijk bijeen te brengen zijn, leidt dit tot ontevredenheid bij de burgers en tot afnemend vertrouwen in de politie en verlies van legitimiteit van de politie. De politie streeft er naar haar functioneren en, daaraan gekoppeld, de beeldvorming voortdurend te optimaliseren. Onderdeel daarvan is het formuleren van een gedeelde, samenhangende opvatting vanuit de professie over wat bijdraagt aan het bevorderen van veiligheid. Dit document bevat de richtinggevende principes van een dergelijke opvatting verwoord in een missie, een visie en een strategie voor de komende jaren.’

(Raad van Hoofdcommissarissen, 2005: 21)

In de nieuwe politiestrategie wordt ‘nodale oriëntatie’ naar voren geschoven als kernconcept. Geïnspireerd op Manuel Castells’ werk over de netwerksamenleving (2000), onderscheidt de politie een ‘space of flows’ naast de ‘space of places’. In de nieuwe strategie concentreert de politie zich op de knooppunten en stromen die samen de ‘space of flows’ vormen. In de woorden van de RvH: ‘De nodale oriëntatie (‘infrastructuurpolitie’) leidt tot toezicht houden op de infrastructuur. Of beter, op de stromen van mensen, goederen, geld en informatie die zich over de infrastructuur verplaatsen’ (Raad van Hoofdcommissarissen, 2005: 90). Om het toezicht op de stromen te realiseren ziet de politie zich genoodzaakt om informatiegestuurde werkmethoden te ontwikkelen en daarbij de uitwisseling van informatie met partners in het veiligheidsdomein zeker te stellen. Deze nadruk op het belang van informatie brengt een manier van werken met zich die meer dan ooit doordrongen is van technologie:

Dit betreft vooral de high tech toepassingen, zoals catch scan-technieken⁴⁹ waarbij waarnemingen en registraties van personen en voertuigen worden vergeleken met uiteenlopende databestanden (bijvoorbeeld openstaande boetes, gestolen voertuigen, vermiste kentekenplaten, bekende verdachten)

(Raad van Hoofdcommissarissen, 2005: 90)

Hiermee wordt ANPR door de landelijke politietop gepresenteerd als prototype technologie voor het realiseren van nodale oriëntatie. De Politie Noodaalsstad maakt de link tussen ANPR en nodale oriëntatie enkele jaren later expliciet, wanneer beleidsmedewerkers van de Dienst Informatie gaan werken aan een eigen interpretatie

⁴⁹Dit is een andere benaming van wat later bekend zou staan als ANPR.

van het landelijk geïntroduceerde concept nodale oriëntatie. In een richtinggevend beleidsdocument over nodale oriëntatie van begin 2008 stelt de Politie Nodaalstad:

‘Het concept nodale oriëntatie lijkt een logische reactie op het waarborgen van veiligheid en het terugdringen van criminaliteit binnen de moderne samenleving. Toch is het nog niet gekomen tot een eenduidige definiëring en inbedding van nodale oriëntatie binnen het politiebestedel. Op operationeel niveau wordt wel steeds vaker technologie ingezet om controle uit te oefenen op infrastructurele knooppunten. Automatic Number Plate Recognition (ANPR) is zo’n technologie die intensief wordt ingezet door de Politie Nodaalstad om controle te houden op vervoersstromen. [...] De Politie Nodaalstad wil vanwege haar voortrekkersrol op het gebied van ANPR en de aanwezigheid van mondiale infrastructurele knooppunten binnen haar werkgebied een bepalende rol vervullen bij de verdere invulling van nodale oriëntatie binnen het politiebestedel.’

In hetzelfde beleidsdocument definieert de Politie Nodaalstad nodale oriëntatie als volgt:

‘Een aanvullende denk- en werkwijze waarbij de politie met behulp van technologie toezicht en controle uitoefent op stromen en knooppunten teneinde veiligheidsrisico’s en strafbaar gedrag zichtbaar te maken om zo effectieve maatregelen te kunnen treffen om de veiligheid binnen de netwerksamenleving te waarborgen en de criminaliteit terug te dringen.’

Technologieassumptie 7:

ANPR draagt bij aan nodale oriëntatie, en daarmee het zichtbaar maken van risico’s.

De Politie Nodaalstad maakt een onderscheid tussen proactieve en reactieve nodale oriëntatie. ‘Dit onderscheid is met name van belang bij de juridische legitimatie van nodale oriëntatie.’, aldus gesteld in het beleidsdocument. Wat is dan het verschil tussen beide? Volgens de Politie Nodaalstad vormen veiligheidsrisico’s en strafbaar gedrag het startpunt van nodale oriëntatie, waarbij er sprake zou zijn van proactieve nodale oriëntatie als de aanleiding slechts een ‘verwachting of aanwijzing’ is en van reactieve nodale oriëntatie ‘als de aanleiding concreter te benoemen is’. In de verdere uitwerking van het onderscheid tussen proactieve en reactieve nodale oriëntatie komt naar voren dat de twee vormen niet alleen een verschillend startpunt hebben, maar vooral verschillende richtpunten. Bij de proactieve werkwijze worden de volgende kenmerken genoemd:

‘Het tijdig signaleren van (potentieel) crimineel gedrag [...] criminaliteit wordt voorkomen (tegengehouden) [...] interventiekansen aan de voorkant van de problematiek [...] De nodale oriëntatie in de proactieve fase heeft dus vooral tot doel om strategische en tactische analyses te kunnen maken en richt zich daarmee op voorspellingen, hotspots en hottimes.’

Technologieassumptie 8:

ANPR draagt bij aan nodale oriëntatie, en daarmee aan preventie van criminaliteit.

Reactieve nodale oriëntatie wordt als volgt gepresenteerd:

‘In een opsporingsonderzoek kan informatie over stromen en knooppunten ook heel nuttig zijn om de dader van een bepaald delict op te sporen. Vooral een nodale oriëntatie naar groepen daders kan waardevolle informatie opleveren. De reactieve nodale oriëntatie heeft tot doel om daderprofielen en operationele analyses te kunnen maken.’

Deze tweedeling tussen proactieve en reactieve nodale oriëntatie zou nuttig zijn voor ‘de begripsvorming van toepassingsmogelijkheden en het opstellen van een juridisch kader’. Tegelijkertijd tornt de Politie Noodaalstad zelf aan de tweedeling door te benadrukken dat er wederzijdse kruisbestuiving kan zijn tussen proactieve en reactieve nodale oriëntatie. Zo ‘kunnen de lessen die geleerd worden uit een reactieve nodale oriëntatie ook nuttig zijn bij het voorkomen en tijdig onderkennen van crimineel gedrag’. Daarna spreekt de Nodaalse politie twijfel uit over de toepasbaarheid van het gemaakte onderscheid en benadrukt nog eens wat de twee vormen met elkaar gemeen hebben:

‘Beide vormen gaan over het signaleren van afwijkend gedrag binnen stromen en knooppunten en maken de kenmerken van criminaliteit en veiligheidsrisico’s inzichtelijk. De kenmerken van criminaliteit en veiligheidsrisico’s kunnen nuttig zijn bij zowel de voorkant (preventie) als de achterkant (reactie) van veiligheidsbeheersing. [...] Toch is het in sommige gevallen lastig om de proactieve variant te scheiden van de reactieve variant. In de praktijk zal moeten blijken waar de scheidslijn ligt en hoe met het tussenliggende grijze gebied moet worden omgegaan.’

De praktische betekenis van nodale oriëntatie verkent de Dienst Informatie in eerste instantie aan de hand van ANPR. Op mijn eerste dag bij hen op kantoor vertellen de betrokken beleidsmedewerkers mij dat ANPR op zichzelf niet de focus heeft. Voor hen

is ANPR slechts één van de vele technieken die in dienst kunnen staan van de nieuwe politiestrategie nodale oriëntatie. Deze techniek vormt voor de Dienst Informatie een bruikbare casus om het korpsbeleid over nodale oriëntatie uit te werken. Tegelijkertijd betekent deze ontwikkeling voor de politiemensen die al met ANPR werken dat een nieuwe beleidsmatige inbedding wordt gecreëerd voor bestaande en nieuwe ANPR-toepassingen. De dienstleiding omschrijft hoe ANPR kan bijdragen aan nodale oriëntatie:

‘Nodale oriëntatie: het idee dat je op knooppunten en stromen informatiestromen moet insteken om helderheid te krijgen in die steeds sneller, digitaler en diffuser wordende wereld, ook vanuit handhavingsoogpunt. Vandaar dat we hebben gezegd: “dat is op zich wel een goed principe”. Vanuit het criminaliteitsaspect wil je als overheid een zekere veiligheid waarborgen, en dat wordt natuurlijk versterkt door het terrorismeaspect. Intussen gaat de wereld steeds sneller, mensen worden steeds mobieler. Hierdoor heb je steeds minder grip vanuit de oude traditionele toezichtsfeer en zul je andere vormen van beheersing moeten realiseren. Nou, daar is ANPR er één van, omdat heel veel dingen mobiliteit nodig hebben. En een belangrijke vorm van mobiliteit zijn auto’s met kentekens. Als je die kunt traceren en kunt analyseren, dan heb je een handig middel om te acteren tegen criminaliteit of tegen ongewenst gedrag. Toen zijn we die op een aantal belangrijke stromen, in feite wegen, gaan plaatsen.’

Legitimiteitsassumptie 10:

De politie moet ANPR inzetten om veiligheid in de veranderde samenleving te kunnen waarborgen.
(normatieve rechtvaardiging)

Technologieassumptie 9:

ANPR draagt bij aan nodale oriëntatie, en daarmee beheersing van de belangrijke knooppunten en stromen in de regio.

Opvallend is dat de introductie van ANPR in Nodaalstad nu wordt gepresenteerd als een doordachte stap in het kader van nodale oriëntatie, terwijl eerder duidelijk is geworden dat ANPR is begonnen als een experiment van de verkeerspolitie. Ook de korpsleiding geeft een nodale herinterpretatie van een eerder uitgevoerde ANPR-toepassing en uit daarnaast de intentie om op basis van het idee van nodale oriëntatie de directe opvolging met ANPR verder door te voeren:

‘Als Bulgaarse en Roemeense criminele groeperingen hit en run criminaliteit plegen, vaak met inbraken, dan is het natuurlijk heerlijk om jouw camera in te stellen van ’s avonds twaalf uur tot een uur of zes de volgende morgen. Daarbij zeggen wij: als er dus twee kentekens van Bulgaarse of Oost-Europese afkomst achter elkaar door dit apparaat heenrijden, dan blijft hij even, want dan gaan wij even kijken wat er aan de hand is. Nou, we hebben daar voorbeelden van, dat dat dus leidt tot de aanhouding van daders. Dan zeg je: wat gebeurt daar nu? Nou zo’n gedacht is gebaseerd op die nodale oriëntatie, op dat fysieke knooppunt. Dat zou in Nodaalstad heel goed kunnen worden voorgesteld: een soort ring waarmee je camera’s systematisch een bepaald type van basisgegevens meegeeft op grond waarvan een reactie komt. Dat kan snelheid zijn of type kentekens of type auto’s of – dan wordt het veel ingewikkelder en interessanter – een bepaalde tenaamstelling van een auto. Als we nou weten dat iemand een crimineel is die altijd inbreekt, dan voeren wij die in. Als hij ’s nachts om 2 uur op de weg zit, dan gaat er een bleepje en zeggen wij: die crimineel zit op ons net. Dan moeten we eens even op pad. Nou dat soort dingen roepen in zo’n Rathenaulezing⁵⁰ ... Ze gooien nog net geen tomaten naar me, maar het is wel heel spannend dan. Het is voor hen onbestaanbaar dat dat gebeurt. En ik ben ervan overtuigd dat dat gebeuren zal.’

Technologieassumptie 10:

Aan de hand van ANPR-hotlists kan de politie mensen uit vervoersstromen selecteren.

Dat de bovengenoemde overtuiging niet op het luchtledige is gebaseerd, ontdek ik tijdens een bezoekje aan de lokale ANPR-divisie. Aldaar vinden ANPR-analyses plaats voor criminaliteitsbestrijding die niet valt onder het traditionele opsporingsonderzoek, waarbij de politie zoekt naar de dader(s) van een gepleegd delict. Het nieuwe type ANPR-analyses draait om het in beeld brengen van vervoerspatronen van bepaalde doelgroepen. Om dit type analyses verder te ontwikkelen, heeft de Politie Nodaalstad begin 2009 een misdaadanalist aangesteld binnen de LAD. Deze analist verricht dus geen analyses voor specifieke opsporingsonderzoeken, maar wel voor problematiek die op de agenda staat van de korpsleiding. De LAD-chef vertelt me dat er op dit moment prioriteit wordt gegeven aan woninginbraken en overvallen. De misdaadanalist laat mij zien met welke opdracht hij op dat moment bezig is: de aanpak van woninginbrekers.

⁵⁰ Lezing bij het Rathenauinstituut.

Omdat het aantal woninginbraken in de regio flink is gestegen, heeft de korpsleiding prioriteit gegeven aan het ontwikkelen en up-to-date houden van een hotlist voor dit delict. Ik kom erachter dat op de hotlist ‘woninginbrekers’ niet alleen woninginbrekers staan. Naast veroordeelde en niet-veroordeelde verdachten staan ook ‘betrokkenen’ en mensen met een ‘aandachtsvestiging’ op de lijst. Deze drie categorieën, verdachte, betrokkene en aandachtsvestiging, zijn standaardcategorieën in het politie-registratiesysteem voor aangiftes. De hotlist met kentekens van ‘woninginbrekers’ wordt wekelijks vernieuwd in de BOF en ook in de mobiele camera-systemen geladen. Bij een wijkscan door een ANPR-auto kunnen dan ook hits voor deze hotlist worden geconstateerd. Een hit kan dan betekenen dat de auto van een veroordeelde woninginbreker wordt gelokaliseerd, maar het kan ook om een getuige (betrokkene) gaan of om iemand die rondom een woninginbraak de aandacht heeft getrokken van de politie. Over de criteria voor inclusie op een hotlist lijkt binnen het korps vooralsnog weinig discussie te bestaan. In een bericht van november 2008 op de ANPR-site binnen het Nodaalse intranet staat vermeld:

‘De hotlists zijn beoordeeld op doelmatigheid, operationele uitvoerbaarheid en juridische haalbaarheid. Op dit moment is het systeem gevoed met ruim 60 verschillende hotlists.’

Legitimiteitsassumptie 11:

De politie mag ANPR-hotlists gebruiken om mensen uit vervoersstromen te selecteren. (legaliteit)

Elders in het land leidt de samenstelling van een hotlist wel degelijk tot discussie, zo vertelt een politiefunctionaris die betrokken is bij de ontwikkeling van landelijk ANPR-beleid:

‘Dat korps zei: “Wij willen ANPR ook wel gebruiken, maar dan koppelen we onze beroepscriminelen daaraan.” Zij gingen die beroepscriminelen uit het verkeer halen en die werden dan even met extra aandacht gecontroleerd. Dat heeft toen nog een boeiend incident opgeleverd, want toen vroeg iemand die voor de derde keer in een week staande was gehouden: “Wat is dat voor een gedoe, dat jullie iedere keer mij staande moeten houden?” Toen zei die agent die controleerde: “Ja, maar u bent een beroepscrimineel.” “Een beroepscrimineel?” Toen kwam er een enorme tegenbeweging vanuit advocaten van die man, maar ook anderen, over hoe de politie er nou bij komt om een bestand aan te leggen van beroepscriminelen. En is dat wel betrouwbaar, gelegitimeerd en gecontroleerd door een derde partij?’

Door dat incident is er wat de klad gekomen in ANPR bij dat korps. Het ANPR-systeem werkte dan nog wel voor dat oude deel, van de directe handhaving, maar voor de opsporing van de werkende beroepscriminelen was het wat in diskrediet geraakt.’

De misdaadanalist licht toe dat hij de hotlist woninginbrekers gebruikt voor analyses om enerzijds verdachten van nieuwe woninginbraken te vinden en anderzijds de pakkans van daders te vergroten. In de begeleidende notitie bij de opzet van een dergelijk onderzoek naar potentiële woninginbrekers lees en zie ik hoe de analist van gegevens tot de benodigde informatie komt:⁵¹ ‘Vanuit de BOF is een overzicht van potentiële woninginbrekers gegenereerd over de periode 23 t/m 29 maart 2009.’ Dit overzicht, een zogenaamd hits report, is een chronologisch geordende lijst met passagegegevens. Onderstaande tabel met fictieve gegevens geeft een indruk van deze lijst.

Technologieassumptie 11:

De politie kan ANPR gebruiken om potentiële criminelen nader te onderzoeken.

Kenteken	Datum/tijd	Hotlist	Cameranaam / richting (camera identifiers)	Latitude / longitude
xx-yy-zz	23/03/09 00:01:01	0001 woninginbrekers	Nodaalweg Zuid Noord Rechts (100: 200:1)	N52:46:52 E005:13:35
pp-ss-tt	23/03/09 01:02:03	0001 woninginbrekers	Nodaalweg Noord Zuid Links (100:200:2)	N52:46:52 E005:13:34

Tabel 7: Fictief hits report

‘Hier kwamen 252 hits naar voren met betrekking tot 46 verschillende voertuigen.’ Een volgende tabel in de onderzoeksopzet geeft voor ieder van de 46 kentekens een overzicht van het aantal passages (hits) per camerale locatie met in de laatste kolom het totale aantal hits in de betreffende week. De lijst is geordend op basis van het totale aantal hits, met de meeste hits bovenaan. In één oogopslag is duidelijk dat één potentiële inbreker met bijna 40 hits beduidend vaker langs Nodaalse ANPR-camera’s

⁵¹ Ik krijg deze onderzoeksopzet na afloop van het betreffende bezoek aan de LAD opgestuurd. De analist en zijn collega hebben het document voor mij geanonimiseerd door naam en kentekengegevens hier uit te knippen.

is gereden dan de andere 45 voertuigen op de lijst. De volgende pagina's geven een 'overzicht incidenten woninginbraak' met daarop per voorval de adresgegevens en de tijdsperiode waarin de gemelde inbraak heeft plaatsgevonden. Op een kaart staan vervolgens de inbraken aangeduid die in het gebied rond de cameralocaties hebben plaatsgevonden. Het vinden van verdachten gebeurt door meldingen van gepleegde inbraken en voertuigbewegingen van de hits in de aan de BOF gekoppelde GIS-applicatiweer te geven. Hierbij wordt ook rekening gehouden met de tijd van de gepleegde inbraken en de tijd waarop voertuigen op de hotlist de vaste cameralocaties passeren om te bepalen welke auto's gekoppeld kunnen worden aan welke inbraken. Deze aanpak past bij de Nodaalse beleidsvisie op nodale oriëntatie:

'Op zich is het analyseren van gegevens en het leggen van relaties tussen diverse gegevensbestanden bij de opsporing niet nieuw. Wel nieuw is de invalshoek dat via stromen en delicten wordt gezocht naar de dader en dat de focus dus niet meer primair ligt op het netwerk van de dader.'

Tegelijkertijd maakt het systeem het ook mogelijk om bepaalde verdachten uit te sluiten, zo licht de misdaadanalist toe. De LAD-chef springt hierop in met een anekdote over iemand die in 2008 één keer verdacht was van een woninginbraak en daardoor op de hotlist terecht was gekomen. Na nader onderzoek bleek deze persoon echter niet betrokken te zijn bij woninginbraken, maar wel bij drugstransacties. Vervolgens is diegene 'losgelaten' wat betreft woninginbraken en op de landelijke hotlist van drugsrunners geplaatst.

Nadere analyse van voertuigbewegingen kan ook informatie opleveren over tijden waarop inbrekers doorgaans langs een vaste cameralocatie komen vóór of na het plegen van een inbraak. *'Wij willen aan de voorkant van het probleem gaan zitten en een kerel snappen met een breekijzer et cetera in de kofferbak.'*, zo vertelt de LAD-chef. In de onderzoeksopzet wordt de hiervoor benodigde analyse van gegevens gedemonstreerd aan de hand van het eerder vermelde voertuig met de meeste hits. In een eerste staafdiagram zijn op de horizontale

as de vier tijdsperioden 0.00-6.00, 6.00-12.00, 12.00-18.00 en 18.00-24.00 uur te zien en op de verticale as het aantal vervoersbewegingen van 23 t/m 29 maart 2009. Hierop staan gekleurde staven per cameralocatie en vervoersrichting afgebeeld. Meteen valt op dat er tussen 6.00 en 12.00 uur geen voertuigbewegingen zijn geregistreerd en dat 15 passages tussen 18.00 en 24.00 uur op één cameralocatie hebben plaatsgevonden,

Technologieassumptie 12:

De politie kan ANPR gebruiken om criminelen tegen te houden.

waarvan zeven van Zuid naar Noord en acht van Noord naar Zuid. In een tweede staafdiagram van dezelfde gegevens zijn de afzonderlijke cameralocaties niet meer te zien, maar zijn de bewegingen van Zuid naar Noord en van Noord naar Zuid geaggregeerd weergegeven. De begeleidende notitie bij de onderzoeksopzet vermeldt dat aan de hand van de twee grafieken ‘kan worden gezien op welke locatie en gedurende welk tijdsblok men de grootste pakkans heeft’. Hierdoor kan de politie gericht agenten inzetten om voertuigen aan te houden en de kans te vergroten om diefstalinstrumentarium of gestolen waar in een kofferbak aan te treffen.

Als laatste onderdeel van de onderzoeksopzet is ‘een persoonsdossier bijgevoegd van de potentiële woninginbreker. Dit om een compleet beeld te geven van de persoon in kwestie’. De betreffende integrale bevraging van de Nodaalse politiebestanden laat zien dat de vermoedelijke bestuurder van het voertuig al meer dan 10 jaar bekend is bij de politie en een reeks antecedenten op zijn naam heeft staan die lang niet allemaal met woninginbraak te maken hebben. Evenwel is de uitgebreide staat van dienst van deze persoon niet de aanleiding voor de analyse van diens vervoersbewegingen, maar is het de combinatie van één toegeschreven kenmerk van deze persoon (potentiële inbreker) en de vervoersbewegingen zelf waarom deze persoon is geselecteerd voor nader onderzoek. Deze aanpak is illustratief voor de toenemende Nodaalse focus op het beteugelen van risico’s, die al naar voren kwam in de definitie van nodale oriëntatie.

‘Je ziet dat wij ons toch bij uitstek gaan richten op degenen die wel een risico vormen voor de maatschappij. En al die anderen die nooit iets misdoen en altijd maar zeer braaf door het leven gaan, waarom zou ik die stoppen? Waarom zou ik die lastigvallen? Nee, dat hoeft helemaal niet.’

(Dienstleiding)

Technologieassumptie 13:

De politie kan ANPR gebruiken om burgers die een risico vormen te selecteren.

De nieuwe invalshoek die nodale oriëntatie biedt voor bestaande en nog te ontwikkelen ANPR-toepassingen geeft een zekere samenhang en richting aan het ANPR-beleid, want ‘ANPR is nodale oriëntatie’. Tegelijkertijd voelt de Politie Nodaalstad de noodzaak om ten behoeve van ‘een brede verantwoorde inzet van nodale oriëntatie’ aandacht te besteden aan de juridische randvoorwaarden en landelijke beleidsontwikkelingen.

3.3.2 Op zoek naar een verantwoorde inzet van ANPR vanuit een nodale oriëntatie

‘Je moet dus de juridische constructie bedenken waarin dat wel kan, op grond waarvan je zo’n instrument toepast in een lokaal of nationaal democratisch stelsel. Het moet dus nooit afhankelijk zijn van het humeur van een politiebaas of hij dat nou wel of niet toepast in al zijn beperkingen die dat kan hebben op het gebied van privacy van mensen. Dus ik loop voortdurend op die twee benen door het leven. Het ene been is: eerst kijken hoe je het nuttige rendement kunt experimenteren, uitontwikkelen, toepassen wat de toegevoegde waarde is op het totaal van je veiligheidsaanpak. En tegelijkertijd transparant zijn en borgen dat dat ook volgens regelgeving plaatsvindt. Met die twee loop je door het leven. Nu eens stap je zo en dan weer stap je zo. Dat is het proces waar wij met de ANPR ook middenin zitten.’

(Korpsleiding)

Met de introductie van nodale oriëntatie begint de Politie Nodaalstad meer samenhang aan te brengen in de verdere ontwikkeling van ANPR-activiteiten. De korps- en dienstleiding willen hiertoe een juridisch kader opstellen en ook aandacht schenken aan het maatschappelijk draagvlak. In eerste instantie ligt de focus in deze beleidsontwikkeling op het vaststellen van een juridisch kader aan de hand van het onderscheid tussen proactieve en reactieve nodale oriëntatie. In tweede instantie verschuift de focus naar de discussie over de balans tussen veiligheid en privacy, die de Politie Nodaalstad breder trekt dan het juridische domein.

Juridische zekerheid door een onderscheid tussen proactieve en reactieve nodale oriëntatie?

In de eerste juridische exercitie concluderen stafmedewerkers van de Dienst Informatie dat er voor het verkrijgen en verwerken van informatie in het kader van reactieve nodale oriëntatie wettelijke grondslagen bestaan in respectievelijk het Wetboek van Strafvordering (opsporings- en verkennend onderzoek) en de Wet Politiegegevens.

Ondanks de aanvankelijke stelligheid over de juridische legitimatie van reactieve nodale oriëntatie, drukken zij zich enkele pagina’s verderop een stuk terughoudender uit als het gaat om de toepasbaarheid van de bevoegdheden voor verkennend onderzoek:

‘Bij een meer reactieve benadering van nodale oriëntatie wordt een specifiek criminaliteitsprobleem “afgepeld” door vanuit de stromen de achterliggende menselijke handelingen inzichtelijk te maken. Zodra er informatie wordt verzameld ten behoeve van een onderzoek naar een specifiek criminaliteitsprobleem, dan is deze informatieverzameling wellicht te scharen onder het regime van het verkennend onderzoek.’

Legitimiteitsassumptie 12:

De politie mag op grond van de Wet Politiegegevens ANPR-analyses uitvoeren ten aanzien van concrete criminaliteitsproblemen. (legaliteit)

In tegenstelling tot een opsporingsonderzoek is er bij een verkennend onderzoek nog geen sprake van een verdachte, maar slechts van aanwijzingen dat binnen een verzameling van personen misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren.⁵² Volgens de Politie Noodalstad is dit artikel dus wellicht van toepassing op reactieve nodale oriëntatie.

Voor proactieve nodale oriëntatie ontbreekt voornamelijk een wettelijke grondslag. In het beleidsdocument wordt de juridische status van deze vorm van nodale oriëntatie als volgt uitgelegd:

‘Steeds vaker gaat de aandacht van justitie en politie uit naar het in een vroegtijdig stadium verzamelen van een grote hoeveelheid gegevens. Dit speelt ook een rol bij nodale oriëntatie in de proactieve fase. Deze vorm van nodale oriëntatie richt zich dan ook tegen onverdachte burgers en een specifieke juridische legitimatie ontbreekt dan ook. [...] De legitimatie voor het verkrijgen van informatie voor proactief onderzoek staat nog ter discussie. Wellicht dat artikel 2 Politiewet een basis kan bieden voor proactieve informatieverkrijging, maar gezien de huidige privacydiscussie lijkt deze grondslag niet afdoende. [...]

⁵² Artikel 126gg Sv luidt: 1. Indien uit feiten of omstandigheden aanwijzingen voortvloeien dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd als omschreven in artikel 67, eerste lid, die gezien hun aard of de samenhang met andere misdrijven die binnen die verzamelingen van personen worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, kan de officier van justitie bevelen dat opsporingsambtenaren daarnaar een onderzoek instellen met als doel de voorbereiding van opsporing. 2. Indien dit noodzakelijk is voor de uitvoering van het onderzoek kan de officier van justitie bepalen dat artikel 9, eerste lid, van de Wet bescherming persoonsgegevens met betrekking tot het onderzoek niet van toepassing is op daarbij nader aan te geven openbare registers die bij wet zijn ingesteld.

Hoewel de nieuwe wet Politiegegevens duidelijk meer armslag biedt voor het verwerken van gegevens, is het niet zo dat de nieuwe wet de weg vrijmaakt voor proactieve gegevensverwerking. De nieuwe wet strekt zich nadrukkelijk alleen uit tot de gerichte vormen van gegevensverwerking.’

In het beleidsdocument maakt de Politie Nodaalstad zelf de brug van het ‘ontbreken van juridische legitimatie’ naar het ‘ter discussie staan van legitimatie’. Vervolgens geeft ze aan actief deel te nemen aan de discussie.

‘De Politie Nodaalstad zal de komende periode de bevoegdheden voor de proactieve variant van nodale oriëntatie verkennen en zal argumenten aandragen ten behoeve van de maatschappelijke en politieke discussie over een eventuele benodigde wetswijziging op dit front. [...] Totdat de uitkomst van de discussie over de balans tussen veiligheid en privacy bekend is, zal de nodale denk- en werkwijze alleen worden toegepast op concrete criminaliteitsproblemen (gerichte analyse). Dit om legitimiteitsproblemen te voorkomen.’

De Politie Nodaalstad kiest voor het verder ontwikkelen van nodale oriëntatie ten aanzien van concrete criminaliteitsproblemen, terwijl ze eerder heeft aangegeven niet zeker te zijn van de juridische grondslag voor het verkrijgen van gegevens voor dit doel. Evenwel blijven de vaste ANPR-camera’s 24 uur per dag gegevens inwinnen. Over de verwerking van ANPR-gegevens ten behoeve van een concreet criminaliteitsprobleem, zoals woninginbraken lijkt de Politie Nodaalstad geen twijfels te hebben. Hiertoe zou de Wet Politiegegevens de juridische grondslag verlenen.

Toch geeft de dienstleiding aan dat er nog veel juridische onduidelikheden bestaan rondom ANPR:

‘Het gaat er niet zozeer om of het al mag of dat het geregeld is, maar het gaat erom of het kan. En dat kunnen, dat is een realiteit. Alleen het beheerst houden, onder welke kaders en regels dat nou mag. Voor een groot deel is dat al geregeld, want een rechter-commissaris mag die gegevens opvragen, de AIVD mag dat doen. Waar het nog niet voor geregeld is, is het gebruik van die gegevens bij proactieve analyses. Of eigenlijk überhaupt analyses an sich. Nou dat is ook niet helemaal waar, want inmiddels is er een aantal praktijksituaties waarbij de regering en de rechter hebben gezegd: “In dit geval mag dat”. Bijvoorbeeld over inbreken bij IJsselland is gezegd: “Dat valt binnen de Politiewet.” Dat is ook een beetje een escape natuurlijk. [...]

Je zult in de toekomst niet alles meer honderd procent in regelgeving heel direct toegesneden kunnen regelen. Dus je zult veel meer regelen in kaderstelling, in toetsing, in algemene formulering. Zoals het Bestuursrecht in redelijkheid en in billijkheid toetst. Dus je kunt niet meer een hele dikke scherpe streep trekken. Je zult die nuances steeds meer gaan moeten afwegen, tussen hoe is het toegepast en wat is de waarde en het belang van de anderen. Of van de maatschappij of van het individu. En in welke mate mag daar nou inbreuk op worden gemaakt.'

De eerste verkenningen van de juridische haken en ogen aan nodale oriëntatie doen de stafmedewerkers concluderen dat 'zowel de doorontwikkeling als de implementatie van nodale oriëntatie afhankelijk zijn van de discussie over de balans tussen veiligheid en privacy'.

Veiligheid en privacy in balans?

Net als enkele jaren eerder, toen het korps zelf een privacyreglement voor ANPR ontwikkelde, neemt de Politie Nodaalstad ook nu geen afwachtende houding aan ten aanzien van juridische en maatschappelijke ontwikkelingen. Het korps gaat zelf op zoek naar een '*balans tussen veiligheid en privacy*', zo getuigt de titel van het beleidsdocument dat twee stafmedewerkers van de Dienst Informatie begin 2009 vervaardigen. In deze zoektocht borduurt de politie voort op de eerdere juridische verkenningen van politiebevoegdheden voor de inzet van technologie en informatie (Wat mag de politie volgens de wet?) en betreft in anticipatie op juridische ontwikkelingen het politiek en maatschappelijk draagvlak hierbij (Wat mag de politie volgens de politiek en burgers, en mogelijk later ook volgens de wet?). Zo komt ze uit op een ruimere interpretatie van zowel artikel 2 Politiewet als de Wet Politiegegevens dan in de eerdere juridische verkenning van nodale oriëntatie:

'Het verkrijgen van informatie over verdachte burgers is geregeld in het Wetboek van Strafvordering. Het verkrijgen van informatie over onverdachte burgers is nog [sic!] niet wettelijk gelegitimeerd. In sommige gevallen wordt artikel 2 Politiewet gebruikt als bevoegdheidsverlenend artikel. Dit is bijvoorbeeld het geval in het antwoord van de Minister van Justitie naar aanleiding van de Kamervragen over de aanvaardbaarheid van het registreren en het gebruiken van kentekens in de regio IJsselland. In dit specifieke geval heeft de minister enige duidelijkheid gegeven. Dit is echter nog niet getoetst door rechterlijke instanties. Voor toekomstige ontwikkelingen van ANPR en voor andere technologische toepassingen is nog helemaal geen uitspraak gedaan. De Politie Nodaalstad gaat er echter vanuit dat de ruimte die de wetgever heeft geboden in de nieuwe Wet Politiegegevens er toe leidt dat de mogelijkheden voor de verbetering van de informatiepositie ook moeten worden verruimd.

De Politie Nodaalstad heeft een aantal richtlijnen opgesteld die zorgen voor een verantwoorde verruiming van de mogelijkheden voor de verbetering van de informatiepositie van de politie. Waar de wettelijke bepalingen rondom de verkrijging van informatie niet duidelijk zijn, geven deze richtlijnen de beoordelingscriteria met betrekking tot de toelaatbaarheid van de verwerking.’

(Beleidsdocument De balans tussen veiligheid en privacy)

Legitimiteitsassumptie 13:

De Politie Nodaalstad mag zelf richtlijnen opstellen voor de omgang met gegevens op basis van een eigen interpretatie van wetgeving. (legaliteit)

Ondanks de uitgesproken bedenkingen over de toepassing van artikel 2 Politiewet⁵³ als bevoegdheidsverlenend artikel, staat dit artikel in het richtinggevend kader prominent vermeld onder het kopje ‘rechtmatige verkrijging gegevens’ in het geval van een ‘beperkte inbreuk op de privacy’. De Politie Nodaalstad baseert deze interpretatie op het Zwolsman-arrest waarbij de Hoge Raad heeft aangegeven dat een geringe privacyinbreuk geen nadere wettelijke bevoegdheid hoeft te hebben. De stafmedewerkers redeneren vervolgens dat de politie bij het verkrijgen van gegevens uitvoering geeft aan de politietaak zoals omschreven in artikel 2 Politiewet en hier voorts geen verdere wettelijke bevoegdheid voor nodig heeft. De ‘rechtmatige verwerking gegevens (= gebruik en bewaren)’ baseert de Politie Nodaalstad volledig op de wet Politiegegevens (Wpolg), waarbij zij opmerkt: ‘Wpolg stelt als voorwaarde voor elke vorm van verdere verwerking dat de verkrijging rechtmatig is’. Intussen blijven de Nodaalse ANPR-camera’s gegevens inwinnen over ‘verdachte’ (hits) en ‘onverdachte’ burgers (no-hits) en blijft de LAD deze bewaren. Opvallend is dat de Politie Nodaalstad in tegenstelling tot in de eerdere juridische verkenning nu van mening is dat de Wpolg, en meer specifiek artikel 10 wel ruimte laat voor proactieve gegevensverwerking:

Legitimiteitsassumptie 14:

De Politie Nodaalstad mag ANPR-gegevens inwinnen, omdat er sprake is van uitvoering van de politietaak bij een geringe inbreuk op de privacy. (legaliteit)

⁵³ Artikel 2 Politiewet 1993: De politie heeft tot taak om in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.

‘Dit artikel is gericht op meer permanente verwerking van gegevens over de betrokkenheid van personen bij het plegen en beramen van zware misdrijven die een ernstige bedreiging vormen voor de rechtsorde. [...] Terrorisme, zware criminaliteit of verstoringen van de rechtsorde door bijvoorbeeld voetbalvandalen vallen onder deze omschrijving. De artikel 10 verwerking gaat dus uit van een proactieve gegevensverwerking ter verbetering van de informatiepositie waarna eventuele maatregelen kunnen worden getroffen.’

Legitimiteitsassumptie 15:

De Politie Nodaalstad mag no-hits analyseren op grond van de Wet Politiegegevens. (legaliteit)

Naast het opstellen van een eigen richtinggevend kader probeert de Politie Nodaalstad zekerheid te krijgen over wat ze mag doen met ANPR door maatschappelijke en politieke ontwikkelingen te volgen en te beïnvloeden:

‘Wat ik wel zie in de landelijke werkgroep juridische kaders ANPR is dat de discussie over de toelaatbaarheid van ANPR wordt gevoerd vanuit drie invalshoeken; politiek-bestuurlijk (hoe past ANPR in het politieke klimaat), pragmatisch (politie; het is zo'n fantastisch middel) en juridisch (past ANPR wel binnen de huidige wettelijke kaders). Volgens mij geeft de optelsom van deze invalshoeken de oplossingsrichting voor het ANPR-vraagstuk. De juristen stellen echter dat de rechtmatigheid het allerbelangrijkste element is bij de vraag of ANPR al dan niet moet worden toegepast in de huidige samenleving.’

(Stafmedewerker)

Het korps heeft vertegenwoordigers in alle nationaal georganiseerde politiewerkgroepen over ANPR. Verschillende informanten geven aan vooral deel te nemen aan deze overleggen om andere politiekorpsen te vertellen hoe zij om zouden moeten gaan met ANPR en om de discussie over juridische normen te beïnvloeden. In het projectplan ANPR derde fase is te lezen:

‘De relatie met het landelijke programmabureau heeft weinig gevolgen voor de verdere uitvoering van het regionale project. Het regionale project voorziet het landelijke programma wel van informatie over hoe zaken opgelost zijn in Nodaalstad.’

De overtuiging dat de Politie Nodaalstad een voortrekkersrol dient te vervullen lees ik ook terug in het beleidsdocument over de balans tussen veiligheid en privacy:

‘De Politie Nodaalstad wordt landelijk gezien als één van de meest innovatieve korpsen in Nederland en schroomt dan ook niet om in de strijd tegen onveiligheid gebruik te maken van nieuwe technologieën en werkwijzen. Het korps Nodaalstad wil dan ook een katalyserende rol spelen bij het ontwikkelen van een beleidsvisie over de inzet van technologie en informatie door de politie.’

Als onderdeel van deze katalyserende rol neemt het korps actief deel aan discussies op de ministeries van BZK en Justitie over nieuwe wetgeving voor ANPR. Zoals een betrokken stafmedewerker het formuleert: *‘We willen voorkomen dat een verdachte voor de rechter staat die ANPR-data beschouwt als onrechtmatig bewijs.’* Daarnaast zie ik dat Nodaalse stafmedewerkers regelmatig onderzoeksrapporten, nieuwsberichten en online burgerforums consulteren. Ze concluderen dat burgers veel belang hechten aan het recht op veiligheid en daarbij innovatie en efficiency verwachten.

Legitimiteitsassumptie 16:

De Politie Nodaalstad mag in het kader van veiligheid de privacy van burgers schenden. (maatschappelijke acceptatie)

Het korps geeft aan zelf het relatieve belang in te schatten van de mening van burgers, maar ook van andere maatschappelijke spelers. Zo vermeldt een stafmedewerker na het doorlezen van een rapport van het College bescherming persoonsgegevens (CBP): *‘Ik ben banger voor het Rathenau instituut’*. Twee Nodaalse leidinggevenden laten zich eveneens uit over de timing en de relevantie van het CBP:

‘Dus je zit aan de ene kant met een toepassingsvraag van: wat betekent het nou eigenlijk? En met de Jacob Kohnstammen, ja ga nou even van mijn rug af, ik kom nog bij jou terug, maar we weten het nog even niet. Totdat de regels zijn gesteld en je die ook zo helder en zo duidelijk mogelijk moet toepassen, daar mag geen twijfel over bestaan. Nou daartussen zit het.’

(Korpsleiding)

‘Die lui zijn echt gek. Dat CBP voert een achterhoedegevecht. En die zijn daar helemaal niet van, die moeten zich bezig gaan houden met waarvan ze van zijn en geen initiërende discussies voeren. Zij zijn degenen die moeten bewaken dat de regels die de politiek stelt, gehandhaafd worden. Dat die niet overtreden worden. Ze moeten zich niet bemoeien met besluitvorming en regelgeving. Daar zijn ze niet van. En ik begrijp het wel, want ze willen zich ook graag profileren en dan ga je dit soort dingen doen. Als je het met dat soort argumentatie moet doen dan ben je eigenlijk een niet serieus te

nemen partner. Het is heel erg stemmingmakend en het is gewoon niet wetenschappelijk, noch serieus. Dus daar heb ik niet zoveel mee. [...] De Tweede Kamer en de gemeenteraad, dat zijn de mensen die uiteindelijk in transparantie de discussie aangaan over wat wel en niet toegepast zou moeten worden. En niet het CBP.'

(Dienstleiding)

Evenwel worden standpunten van het CBP en zijn frontman Jacob Kohnstamm wel besproken in verschillende Nodaalse beleidsdocumenten en luistert de Politie Nodaalstad wel naar deze – in hun ogen – minder relevante actor. Dit lijkt echter vooral een symbolische actie te zijn, die weinig invloed heeft op de Nodaalse beleidsontwikkeling. Beleidsmedewerkers geven hierbij aan dat dit naar de buitenwereld toe wel het beeld versterkt van een politie die belang hecht aan maatschappelijke ontwikkelingen.

Een andere manier waarop de Politie Nodaalstad de beeldvorming beïnvloedt, is een conservatief communicatiebeleid. Er komen persberichten uit over de toepassingen in het kader van verkeershandhaving, maar hierin zijn geen details te vinden over de technologie.⁵⁴ In deze berichten wordt met name aandacht besteed aan de resultaten van bepaalde politieacties, zoals hoeveel boetes er zijn geïnd op een bepaalde locatie. Er bestaat weliswaar enige berichtgeving over ANPR-toepassingen in de criminaliteitsbestrijding, maar slechts in zeer algemene termen en in reactie op vragen van de media. Volgens een stafmedewerker is er hierbij sprake van strikte orders vanuit de korpsleiding.

Naast een verbreding van de vraag 'Wat mag de politie?', voegt de Politie Nodaalstad een andere vraag toe aan de discussie: 'Wat moet de politie?':

'De uitdagingen in de huidige samenleving zorgen ervoor dat de Politie Nodaalstad door wil (moet) gaan met de ontwikkeling van technologische toepassingen en nieuwe werkwijzen.'

(Beleidsdocument De balans tussen veiligheid en privacy)

Zo gesteld *kan* de Politie Nodaalstad niet anders dan investeren in de verdere ontwikkeling van ANPR. Hiermee vindt een subtiele verschuiving plaats in de discussie over ANPR. De eerdere focus op het nut lijkt plaats te maken voor een focus op de noodzaak van ANPR. Niet alleen is ANPR nuttig voor de politie, maar ook nodig, zo wordt duidelijk uit de woorden van de korpsleiding:

⁵⁴ Deze heb ik via het intranet van Politie Nodaalstad kunnen raadplegen.

‘Objectief is er geen speld tussen te krijgen dat het gewoon meer dan een kwart veiliger geworden is, maar niemand voelt dat zo. Niemand. Dus dan kom je op het subjectieve element. [...] Mensen moeten het idee hebben dat je technisch innoveert. Dus dat je alles uit de kast haalt in technische zin, om het veiliger te maken. En dat heeft invloed op het vertrouwen en dat vertrouwen heeft invloed op het subjectieve gevoel van veiligheid. Dus mijn achterliggende strategie is dat ik, naast die objectieve veiligheid, die vanzelfsprekend altijd leidend is hier, heel hard werk aan de beïnvloeding van veiligheid onder meer door technische innovaties toe te passen. Dat is de achtergrond. [...] Ik kan niet tegengaan dat wij in een informatiemaatschappij leven en dat je in 3 seconden de hele wereld langs krijgt, maar wel laten zien dat wij én professioneel, én state-of-the-art zijn als het om innovaties en technische toepassingen gaat. Het is dus geen toeval dat wij op veel van die terreinen aan het pionieren zijn. ANPR is daarin een middel.’

Verder grijpt de Politie Nodaalstad terug op het rapport *Politie in ontwikkeling*, waarin de Raad van Hoofddcommissarissen stelt dat ‘signalering en advisering’ als kerntaak moet worden toegevoegd aan het rijtje van handhaving, opsporing en hulpverlening. In het beleidsdocument *De balans tussen veiligheid en privacy* verbindt het korps deze nieuwe kerntaak aan proactieve informatievergaring:

‘Signaleren en adviseren heeft een proactief element in zich. [...] Proactief politiewerk is gericht op het tijdig signaleren van (potentieel) crimineel gedrag. Het resultaat van het proactieve politiewerk is dat criminaliteit wordt voorkomen (preventie) of dat de controle moet worden geïntensiveerd. [...] Proactief politiewerk vraagt om het verzamelen van informatie over onverdachte burgers.’

Legitimiteitsassumptie 17:

De Politie Nodaalstad moet ANPR proactief inzetten om de politietaak te kunnen vervullen. (maatschappelijke acceptatie)

Volgens een stafmedewerker kan de proactieve werkwijze de politie wellicht ontlasten omdat er dan minder reactief politiewerk zou komen. *‘Nu kunnen ongeveer twee van de tien zaken of meldingen worden aangepakt’*. Een waarde van proactieve inzet van ANPR zou dus efficiencywinst kunnen zijn, zo betoogt ook de dienstleiding:

‘Eigenlijk zou dat een standaardvraag moeten zijn. Als crimineel A met die auto rijdt of met die auto’s, haal ze een keer door de bak heen, want dan heb je in ieder geval een indicatie van wat zijn bewegingen zijn. Als je hem iedere keer om 10 uur ’s avonds door de Nodaallaan ziet rijden. Nou ja, als je hem zoekt, kan je daar ook een keer gaan staan natuurlijk. Hè, dus je bent veel efficiënter en effectiever met je politievak bezig.’

Legitimiteitsassumptie 18:

ANPR is goed, omdat het de politie efficiënter en effectiever maakt.
(normatieve rechtvaardiging)

Voor de meeste informanten is het evident dat ANPR nu al ten goede komt aan de effectiviteit en efficiëntie van het politiekorps en dat deze effecten alleen maar zullen toenemen met de uitgebreidere toekomstige applicaties. Zowel in interviews als in documenten wijzen zij vaak op de behaalde successen in de handhaving om dit effectiviteitsargument vervolgens te gebruiken om toekomstige ANPR-toepassingen te legitimeren. Een ander argument om nieuwe ANPR-toepassingen te rechtvaardigen is een verwijzing naar het concept ‘nodale oriëntatie’.

Legitimiteitsassumptie 19:

ANPR is goed, omdat het nodale oriëntatie is.
(normatieve rechtvaardiging)

Zowel politiefunctionarissen in het veld als beleidsmedewerkers noemen dit vaak bij wijze van rechtvaardiging. *‘ANPR is efficiënt, het is effectief en natuurlijk is het nodale oriëntatie’*. De meeste informanten noemen nodale oriëntatie echter zonder duidelijk uit te leggen wat het inhoudt en waarom het van belang is.

Op het moment dat ik het veldonderzoek afsluit, is de LAD volop de analyse-mogelijkheden met ANPR aan het verkennen en zien de beleidsmedewerkers geen reden om de ingezette koers te wijzigen. Voor de Politie Nodaalstad is het wachten op de definitieve politieke en juridische legitimatie van hun beleid. Gezien de verrichte verkenningen naar de balans tussen veiligheid en privacy is het korps daar zeer hoopvol over gestemd.

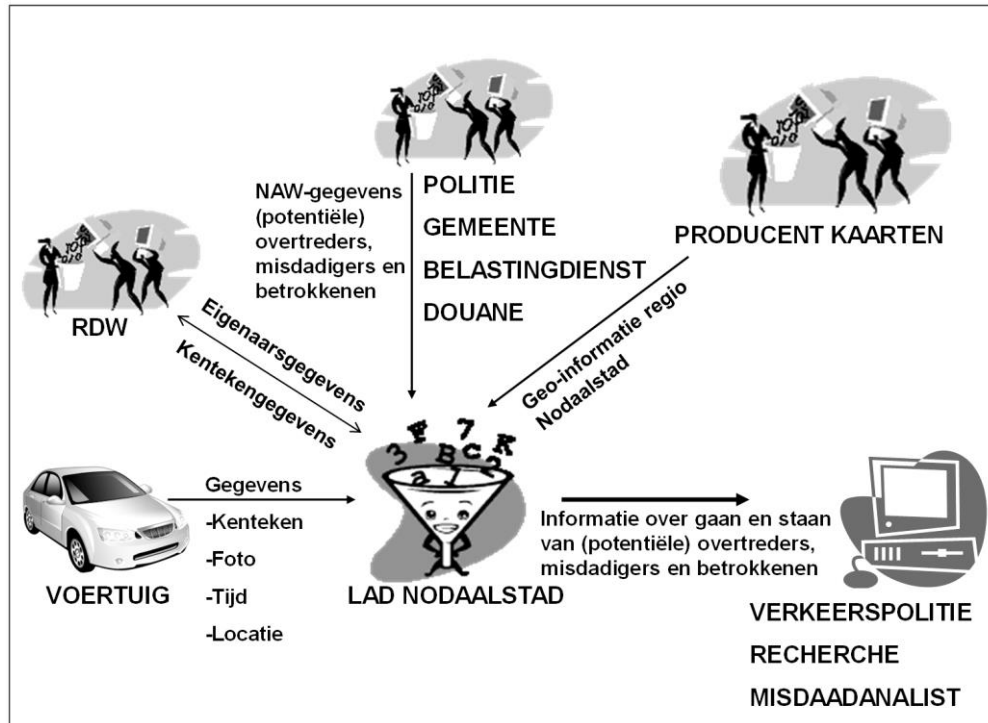
3.4 Recapitulatie

ANPR krijgt op drie manieren betekenis in de beleidspraktijk van de Politie Nodaalstad: in handavings- en opsporingsprocessen en als onderdeel van nodale

oriëntatie. Vanaf 2006 wordt ANPR ingezet als handhavingsinstrument, waarbij overtreders en criminelen op basis van hotlists realtime worden gesignaleerd en uit het verkeer gehaald. Deze toepassing breidt in de loop der jaren door een toename aan ANPR-apparatuur, hotlists en ingezette manuren zowel qua signalering als daadwerkelijke opvolging uit.

In de loop van 2008 raakt ANPR ook ingeburgerd als onderdeel van het opsporingsproces, waarbij ANPR-data als standaard informatiebron en voor aanvullende analyses worden geraadpleegd. Tegelijkertijd ontwikkelt de Politie Nodaalstad beleid om te gaan werken volgens een nodale oriëntatie, waarmee enerzijds een context wordt geboden aan de reeds geïmplementeerde ANPR-activiteiten en anderzijds initiatieven worden ontplooid voor nieuwe toepassingen.

Nodale oriëntatie geeft dan ook een nieuwe betekenis aan bestaande toepassingen. Verkeershandhaving verwordt tot het ingrijpen in verkeersstromen en opsporing wordt het analyseren van knooppunten van informatie. Daarnaast stimuleert nodale oriëntatie een uitbreiding van de politietaak door de aandacht voor het voortijdig ingrijpen op knooppunten en stromen. Wat betreft ANPR komt deze heroriëntatie tot uiting in het ontwikkelen van projecties van verwacht reisgedrag van bepaalde criminelen op basis van historische ANPR-data. Figuur 5 illustreert welke actoren en gegevensstromen een rol spelen bij het genereren van mobiliteitsinformatie met het Nodaalse ANPR-systeem.



Figuur 5: Actoren en gegevensstromen ANPR Politie Nodaalstad

Het ANPR-systeem stelt de politie in staat om mobiliteitsgegevens over burgers in te winnen, te koppelen en te analyseren. Wat is er vanuit informatietechnologisch perspectief te zeggen over het surveillanceobject?⁵⁵ Een optische sensor gecombineerd met satelliettechniek (GPS) wint plaats-, tijds- en objectgegevens in. Op het niveau van inwinning is het surveillanceobject een artefact: de kentekenplaat. Op het niveau van koppeling met een hotlist is het object een (in (politie)bestanden geregistreerde door de voertuigeigenaar in het verleden verrichte) actie: bijvoorbeeld drugsrunnen of dronken besturen. Bij de analyse en interpretatie van gegevens kan het object zowel een actie als een persoon zijn, zo is duidelijk geworden in de paragrafen 3.2 en 3.3. Tabel 8 geeft een overzicht van de mobiliteitsgegevens die worden gegenereerd bij de toepassing van ANPR door de Politie Nodaalstad.

⁵⁵ Zie hoofdstuk 2 voor een nadere toelichting op het begrip surveillanceobject.

Objectgegevens	
Artefact (Apparaatgegevens)	<ul style="list-style-type: none"> - Foto kentekenplaat - Alfabetieke data kentekenplaat
Lichaam (Persoonsgegevens)	<ul style="list-style-type: none"> - Persoonsgegevens voertuigeigenaar
Actie (Situationele identiteit)	<ul style="list-style-type: none"> - Overtreder - Misdadiger - Betrokkene - Aandachtsvestiging - (soms in combinatie met opvallende locatie- en tijdsgegevens)
Locatiegegevens	
Ruimtelijk (Coördinaten)	<ul style="list-style-type: none"> - GPS-gegevens cameralocatie
Netwerk (Cell-topologie)	<ul style="list-style-type: none"> - Geen
Beschrijvend (Geografische verwijzing)	<ul style="list-style-type: none"> - Naam cameralocatie
Tijdsgegevens	
Heden (Realtime ingewonnen gegevens)	<ul style="list-style-type: none"> - Hits t.b.v. geplande ANPR-acties - Hits zware delicten t.b.v. ongeplande directe opvolging
Verleden (Opgeslagen gegevens)	<ul style="list-style-type: none"> - Alle passagegegevens (4 maanden) - Passagegegevens verwerkt in het kader van handhaving rechtsorde (6 maanden)
Toekomst (Gecalculeerde gegevens)	<ul style="list-style-type: none"> - Verwachte passages bekende delinquenten

Tabel 8: Mobiliteitsgegevens bij de toepassing van ANPR

De Politie Nodaalstad vraagt zich vanaf 2007 expliciet af wat ze kan, mag en moet doen met ANPR, zo komt naar voren in interviews en beleidsdocumenten. De discussie over de grenzen van ANPR komt rond die tijd op gang, omdat het korps het arsenaal aan ANPR-apparatuur flink uitbreidt en zich oriënteert op analysetoepassingen die tot op dat moment nog niet gebruikelijk zijn. Over de legitimiteit van ANPR voor verkeershandhaving maakt de politie zich geen zorgen, omdat deze toepassing zich naar haar idee binnen wettelijke kaders afspeelt, op weinig weerstand stuit onder burgers en bovendien haar effectiviteit en efficiency vergroot. De uitbreiding van

ANPR-toepassingen in 2007 daarentegen zorgt bij de Politie Nodaalstad voor grote onduidelijkheid op legitimiteitsgebied. Het is op dat moment alles behalve zeker in hoeverre nieuwe toepassingen wettelijk gelegitimeerd zijn. In eerste instantie verkent de politie daarom vooral het juridisch kader, maar laat in latere rapporten ook beschouwingen zien over het maatschappelijk draagvlak en reacties vanuit de politiek. Ook in andere gremia is de Politie Nodaalstad actief aanwezig. Zo heeft ze vertegenwoordigers in alle nationaal georganiseerde politiewerkgroepen over ANPR. Redenen voor deelname aan deze overleggen zijn om andere politiekorpsen te vertellen hoe zij om zouden moeten gaan met ANPR en om de discussie over juridische normen te beïnvloeden. In deze zoektocht naar legitimiteit voert de Politie Nodaalstad het argument aan dat zij door de proactieve inzet van ANPR de taak om de veiligheid van de veranderende samenleving te waarborgen, beter kan gaan vervullen. Tegelijkertijd voelt zij de noodzaak om succesverhalen te vinden om dit argument te kunnen onderbouwen.

4 Analyse: surveillanceperspectieven in het ANPR-beleid van de Politie Nodaalstad

4.1 Technologie- en legitimiteitsassumpties

Welke beleidsmatige mogelijkheden ziet de Politie Nodaalstad met betrekking tot ANPR? Wat ANPR kan betekenen voor de taakuitoefening van de Politie Nodaalstad, hangt zowel af van de technische mogelijkheden en beperkingen die de politie toedicht aan ANPR (technologieassumpties), als van haar ideeën over wat een legitieme inzet van de technologie inhoudt (legitimiteitsassumpties). Tot dusver is duidelijk geworden dat de Politie Nodaalstad in de ontwikkeling van het ANPR-beleid aandacht besteedt aan diverse wetten, regels en procedures, de inzet van ANPR aan de hand van een aantal (morele) waarden rechtvaardigt en de mening van burgers en autoriteiten op een aantal punten van belang acht. Tabel 9 geeft een overzicht van de dertien technologie-assumpties en negentien legitimiteitsassumpties die in de loop van dit hoofdstuk aan het licht zijn gekomen.

De gevonden technologie- en legitimiteitsassumpties vergelijk ik met de technologie- en legitimiteitsassumpties die ik in hoofdstuk 4 per theoretisch surveillanceperspectief heb vastgesteld. Hierdoor wordt inzichtelijk op welke punten het beleid van de Politie Nodaalstad kenmerken vertoont van de drie surveillanceperspectieven controle, interactie en voorzorg.

Technologieassumpties

1. ANPR heeft een nog nader te bepalen nut voor de politie.
2. ANPR kan zorgen voor beheersing.
3. ANPR verhoogt de pakkans van criminelen en overtreders.
4. Door ANPR kunnen criminelen niet ongezien de regiogrenzen overschrijden (ring of steel).
5. Met ANPR kan de politie de bewegingen van een geselecteerd voertuig reconstrueren.
6. ANPR kan helpen om verdachte voertuigen te identificeren in vervoersstromen.
7. ANPR draagt bij aan nodale oriëntatie, en daarmee het zichtbaar maken van risico's.
8. ANPR draagt bij aan nodale oriëntatie, en daarmee aan preventie van criminaliteit.
9. ANPR draagt bij aan nodale oriëntatie, en daarmee beheersing van de belangrijke knooppunten en stromen in de regio.
10. Aan de hand van ANPR-hotlists kan de politie mensen uit vervoersstromen selecteren.
11. De politie kan ANPR gebruiken om potentiële criminelen nader te onderzoeken.
12. De politie kan ANPR gebruiken om criminelen tegen te houden.
13. De politie kan ANPR gebruiken om burgers die een risico vormen te selecteren.

Legitimiteitsassumpties

1. Voor toegang tot ANPR-gegevens van gemeentecamera's is bestuurlijke toestemming nodig. (maatschappelijke acceptatie)
2. De politie mag ANPR gebruiken, omdat het de uitvoering van de politietaak betreft. (legaliteit)
3. ANPR is legitiem op grond van kenbaarheid van enkele kenmerken van het systeem. (maatschappelijke acceptatie)
4. Het is goed dat de politie ANPR inzet, omdat ze hierdoor efficiënter werkt met minder overlast voor onschuldige/onverdachte burgers. (normatieve rechtvaardiging)
5. Er zijn grenzen aan de categorieën burgers waar de politie de privacy van mag schenden met ANPR. (normatieve rechtvaardiging)
6. De politie heeft een juridische grondslag nodig voor het bewaren van ANPR-gegevens. (legaliteit)
7. Het bewaren van ANPR-gegevens is nodig voor de moderne criminaliteitsbestrijding. (normatieve rechtvaardiging)
8. De politie is genoodzaakt ANPR te gebruiken om de politietaak nog te kunnen uitvoeren in de veranderde samenleving. (normatieve rechtvaardiging)
9. De politie mag ANPR gebruiken in de opsporing op grond van jurisprudentie. (legaliteit)
10. De politie moet ANPR inzetten om veiligheid in de veranderende samenleving te kunnen waarborgen. (normatieve rechtvaardiging)

Legitimiteitsassumpties

11. De politie mag ANPR-hotlists gebruiken om mensen uit vervoersstromen te selecteren. (legaliteit)
12. De politie mag op grond van de Wet Politiegegevens ANPR-analyses uitvoeren ten aanzien van concrete criminaliteitsproblemen. (legaliteit)
13. De Politie Nodaalstad mag zelf richtlijnen opstellen voor de omgang met gegevens op basis van een eigen interpretatie van wetgeving. (legaliteit)
14. De Politie Nodaalstad mag ANPR-gegevens inwinnen, omdat er sprake is van uitvoering van de politietaak bij een geringe inbreuk op de privacy. (legaliteit)
15. De Politie Nodaalstad mag no-hits analyseren op grond van de Wet Politiegegevens. (legaliteit)
16. De Politie Nodaalstad mag in het kader van veiligheid de privacy van burgers schenden. (maatschappelijke acceptatie)
17. De Politie Nodaalstad moet ANPR proactief inzetten om de politietaak te kunnen vervullen. (maatschappelijke acceptatie)
18. ANPR is goed, omdat het de politie efficiënter en effectiever maakt. (normatieve rechtvaardiging)
19. ANPR is goed, omdat het nodale oriëntatie is. (normatieve rechtvaardiging)

Tabel 9: Technologie- en legitimiteitsassumpties in het ANPR-beleid van de Politie Nodaalstad

4.2 Koppeling aan surveillanceperspectieven

4.2.1 Kenmerken van het controleperspectief in het ANPR-beleid van de Politie Nodaalstad

Het controleperspectief is sterk aanwezig in het Nodaalse ANPR-beleid. Ik vind bevestiging van één van beide technologieassumpties en van beide aan dit perspectief toebehorende legitimiteitsassumpties. Ik bespreek de bevindingen per assumptie.

Technologieassumptie: wijdverspreide controle van burgers

Het controleperspectief gaat ervan uit dat surveillancetechnologie de overheid de mogelijkheid geeft om burgers wijdverspreid te controleren op afwijkend gedrag door in de rol van kijker zoveel mogelijk gegevens over zo veel mogelijk burgers als bekeken in te winnen en te verwerken. Deze technologieassumptie manifesteert zich door de volgende veronderstellingen in het ANPR-beleid van de Politie Nodaalstad:

- ANPR kan zorgen voor beheersing.
- ANPR draagt bij aan nodale oriëntatie, en daarmee beheersing van de belangrijke knooppunten en stromen in de regio.
- Door ANPR kunnen criminelen niet ongezien de regiogrenzen overschrijden (ring of steel).
- Met ANPR kan de politie de bewegingen van een geselecteerd voertuig reconstrueren.
- ANPR kan helpen om verdachte voertuigen te identificeren in vervoersstromen.
- Aan de hand van ANPR-hotlists kan de politie mensen uit vervoersstromen selecteren.

Op basis van deze veronderstellingen verruimt de politie de grenzen van het ANPR-dekkingsgebied steeds verder door meer camera's te plaatsen in de buitengebieden van de regio en maakt ze tegelijkertijd het dekkingsgebied fijnmaziger door toegang te verkrijgen tot ANPR-gegevens van de gemeente. Er is een duidelijk streven om zoveel mogelijk ANPR-gegevens in te winnen en op te slaan vanuit de veronderstelling dat afwijkend gedrag gedetecteerd kan worden, wat de politie het idee geeft van beheersing. Hiertoe maakt de politie gebruik van een tweedeling tussen hits (afwijkend gedrag) en no-hits (normaal gedrag). In de loop der jaren wordt de panoptische blik en daarmee de kans om afwijkend gedrag te detecteren om twee redenen steeds groter. Ten eerste heeft de politie überhaupt steeds meer 'gedragsgegevens' (passagegegevens) tot haar beschikking. Ten tweede wordt steeds meer gedrag in het ANPR-systeem als afwijkend bestempeld door een toename aan hotlists (afwijkende surveillanceobjecten) en vanuit de opsporing meer aandacht voor vervoersbewegingen an sich (afwijkende bewegingen).

Technologieassumptie: disciplineren van burgers

Uit het casusmateriaal volgen geen aanwijzingen dat de politie veronderstelt dat ANPR de mogelijkheid zou geven om burgers te disciplineren. Weliswaar is het korps vrij terughoudend met het naar buiten toe verstrekken van meer dan oppervlakkige informatie over de toepassing van ANPR, maar dit is niet gemotiveerd vanuit de gedachte om burgerlijke gehoorzaamheid af te dwingen door burgers in het ongewisse te laten over hoe en wanneer ze onder controle staan. De voorzichtige communicatie heeft vooral te maken met angst voor een rem op ANPR-ontwikkelingen door een mogelijke aantasting van legitimiteit.

Legitimiteitsassumptie: inzet van surveillance ten aanzien van burgers

De casus laat zien dat de Politie Nodaalstad in haar beleidsvorming aandacht besteedt aan de juridische, ethische en maatschappelijke gronden waarop het beheersinstrument ANPR wordt ingezet. Deze legitimiteitsassumptie manifesteert zich door de volgende veronderstellingen in het ANPR-beleid van de Politie Nodaalstad:

Legaliteit

- De politie mag ANPR gebruiken, omdat het de uitvoering van de politietaak betreft.
- De politie mag ANPR-hotlists gebruiken om mensen uit vervoersstromen te selecteren.
- De politie mag op grond van de Wet Politiegegevens ANPR-analyses uitvoeren ten aanzien van concrete criminaliteitsproblemen.
- De Politie Nodaalstad mag zelf richtlijnen opstellen voor de omgang met gegevens op basis van een eigen interpretatie van wetgeving.
- De politie mag ANPR gebruiken in de opsporing op grond van jurisprudentie.

Normatieve rechtvaardiging

- De politie is genoodzaakt ANPR te gebruiken om de politietaak nog te kunnen uitvoeren in de veranderde samenleving.
- Het bewaren van ANPR-gegevens is nodig voor de moderne criminaliteitsbestrijding.
- De politie moet ANPR inzetten om veiligheid in de veranderende samenleving te kunnen waarborgen.
- ANPR is goed, omdat het de politie efficiënter en effectiever maakt.
- ANPR is goed, omdat het nodale oriëntatie is.

Maatschappelijke acceptatie

- ANPR is legitiem op grond van kenbaarheid van enkele kenmerken van het systeem.

Aan de hand van deze veronderstellingen legitimeert de Politie Nodaalstad voor zichzelf en naar buiten toe dat ANPR steeds breder wordt ingezet. Hierbij valt op dat het korps legaliteit en maatschappelijke acceptatie beziet als bevoegdheidsverlenende aspecten van legitimiteit (Wat mag de politie?) en de normatieve rechtvaardiging vooral betrekking heeft op de taakstelling van de politie (Wat moet de politie?).

Legitimiteitsassumptie: beschermen van privacy van burgers

Ook de bescherming van de privacy van burgers krijgt aandacht in de beleidsvorming, zij het beduidend minder uitgebreid dan de gronden voor de inzet van ANPR. De assumptie dat aandacht voor privacy van belang is bij de inzet van surveillance komt als volgt tot uiting:

Legaliteit

- De Politie Nodaalstad mag ANPR-gegevens inwinnen, omdat er sprake is van uitvoering van de politietaak bij een geringe inbreuk op de privacy.
- De politie heeft een juridische grondslag nodig voor het bewaren van ANPR-gegevens.

Maatschappelijke acceptatie

- De Politie Nodaalstad mag in het kader van veiligheid de privacy van burgers schenden.

Opvallend is dat er met name aandacht is voor de juridische dimensie van privacy en niet voor de normatieve dimensie. De politie vraagt zich dus wel af wat een inbreuk op privacy juridisch gezien betekent en onder welke voorwaarden deze plaats mag vinden, maar stelt niet de vraag of en in welke situaties dit een goede of slechte zaak zou zijn.

4.2.2 Kenmerken van het interactieperspectief in het ANPR-beleid van de Politie Nodaalstad

Het interactieperspectief is amper aanwezig in het Nodaalse ANPR-beleid. Ik constateer een geringe aanwezigheid van beide legitimiteitsassumpties, en niet van de technologieassumpties. Ik bespreek de bevindingen per assumptie.

Technologieassumptie: verbinden van overheid en burgers

Dat surveillancetechnologie overheid en burgers met elkaar in verbinding zou kunnen brengen, komt niet terug in het Nodaalse ANPR-beleid. De politie beziet burgers vanuit de lokale ANPR-divisie eerder vanaf een afstand. Wel zoekt en vindt het korps nieuwe verbindingen met andere overheidsinstanties.

Technologieassumptie: gezamenlijke informatiecreatie

Surveillancetechnologie stelt overheid en burgers in staat om informatie over zichzelf en elkaar te creëren, te beoordelen en aan te passen, zo luidt deze assumptie. Ook deze technologieassumptie komt niet tot uiting in het ANPR-beleid. De politie gaat puur en alleen uit van de informatie uit het eigen ANPR-systeem en databases van andere overheidsorganisaties en ziet burgers niet als producenten van die informatie. Vervolgens is ze niet geïnteresseerd in het creëren van mogelijkheden voor burgers om gegevens in te zien, te beoordelen of aan te passen.

Legitimiteitsassumptie: toegang tot surveillance-informatie

Op welke gronden politiefunctionarissen toegang krijgen tot de BOF, de database met ANPR-gegevens wordt niet geproblematiseerd in de beleidsvorming. Bepaalde functionarissen hebben directe toegang tot de gegevens en anderen dienen informatieverzoeken in die worden beoordeeld door medewerkers van de LAD. Hierbij is sprake van een status quo waarvan de legaliteit, normatieve rechtvaardiging of maatschappelijke acceptatie niet ter discussie staan binnen het korps. Wel is er in de beleidsvorming aandacht voor het verkrijgen van structurele toegang tot ANPR-gegevens die zijn ingewonnen door gemeentecamera's:

Maatschappelijke acceptatie

- Voor toegang tot ANPR-gegevens van gemeentecamera's is bestuurlijke toestemming nodig.

Evenwel gaat de discussie over het gebruik van de gemeentelijke ANPR-gegevens veel meer over privacy dan over de maatschappelijke acceptatie van politietoegang tot de gegevens.

Legitimiteitsassumptie: relevantie en kwaliteit van surveillance-informatie

De kwaliteit van ANPR-gegevens en hotlists staat grotendeels buiten kijf in het Nodaalse ANPR-beleid. Alleen vanuit de opsporing zijn wat geluiden te horen dat ze graag duidelijkere camerabeelden zouden hebben, maar is er tegelijkertijd begrip voor dat het ANPR-systeem is gericht op het herkennen van kentekens en niet de inzittenden. In het ANPR-beleid is wel aandacht voor de juridische beoordeling van de relevantie van ANPR-informatie, en meer specifiek de no-hits.

Legaliteit

- De Politie Nodaalstad mag no-hits analyseren op grond van de Wet Politiegegevens.

4.2.3 Kenmerken van het voorzorgperspectief in de beleidspraktijk

Het voorzorgperspectief manifesteert zich op een aantal punten in het Nodaalse ANPR-beleid. Ik vind bevestiging van alle technologie- en legitimiteitsassumpties en bespreek de bevindingen per assumptie.

Technologieassumptie: identificeren van risico's en risicoburgers

De aanname dat surveillancetechnologie de mogelijkheid geeft om risico's en risicoburgers te identificeren, komt in één technologieassumptie naar voren:

- ANPR draagt bij aan nodale oriëntatie, en daarmee het zichtbaar maken van risico's.

De politie is overtuigd van de potentie van het ANPR-systeem om proactief risico's in beeld te brengen, maar gebruikt het systeem in de praktijk (nog) niet als zodanig. Er wordt geen datamining toegepast om vanuit de BOF nog onbekende risico's naar boven te halen.

Technologieassumptie: beteugelen van risico's

Deze tweede technologieassumptie binnen het voorzorgperspectief komt sterker tot uiting dan de eerste. In de ogen van de politie geeft ANPR de mogelijkheid om risico's te beteugelen door bepaalde groepen burgers extra in de gaten te houden. De volgende beleidsveronderstellingen wijzen hierop:

- De politie kan ANPR gebruiken om burgers die een risico vormen te selecteren.
- ANPR draagt bij aan nodale oriëntatie, en daarmee aan preventie van criminaliteit.
- De politie kan ANPR gebruiken om potentiële criminelen nader te onderzoeken.
- De politie kan ANPR gebruiken om criminelen tegen te houden.
- ANPR verhoogt de pakkans van criminelen en overtredders.

Deze veronderstellingen liggen ten grondslag aan de beleidsontwikkeling van aanhouden naar tegenhouden. In de loop der jaren richt de politie zich naast het

detecteren en aanhouden van burgers die een overtreding of misdaad hebben begaan op mogelijkheden voor het detecteren en tegenhouden van burgers die wel eens iets kunnen gaan doen wat een risico vormt voor de veiligheid. De definitie van risico's wordt hierbij gemaakt door de korpsleiding en de vertaling naar risicoburgers door de LAD. Het ANPR-systeem wordt voorts gebruikt voor het specificeren van al bekende risico's en levert zo de informatiebasis voor een politie-interventie in het veld.

Legitimiteitsassumptie: definiëring van risico's en risicocategorieën burgers

De Politie Nodaalstad besteedt in haar beleidsvorming weinig aandacht aan de gronden waarop risico's en risicocategorieën burgers worden gedefinieerd. Ik tref geen veronderstellingen aan over de legaliteit van de keuze van de korpsleiding voor het verkennen van een bepaald risico, noch voor de zoekcriteria die de LAD-analist gebruikt om risicoburgers in beeld te brengen. Wel is de normatieve rechtvaardiging en maatschappelijke acceptatie van belang in het ANPR-beleid:

Normatieve rechtvaardiging

- Er zijn grenzen aan de categorieën burgers van wie de politie de privacy mag schenden met ANPR.
- Het is goed dat de politie ANPR inzet, omdat ze hierdoor efficiënter werkt met minder overlast voor onschuldige/onverdachte burgers.

Maatschappelijke acceptatie

- De Politie Nodaalstad moet ANPR proactief inzetten om de politietaak signalering en advisering te kunnen vervullen.

Op basis van deze veronderstellingen gaat de politie door met het verkennen van de tactische en operationele betekenis van en legitieme mogelijkheden voor een proactieve inzet van ANPR.

4.2.4 Overzicht van surveillanceperspectieven in het ANPR-beleid van de Politie Nodaalstad

Het ANPR-beleid van de Politie Nodaalstad vertoont kenmerken van zowel het controleperspectief als het voorzorgperspectief. Het interactieperspectief drukt nauwelijks een stempel op het ANPR-beleid. Tabel 10 geeft een overzicht van de analyse van surveillanceperspectieven in het ANPR-beleid van de Politie Nodaalstad.

Technologie- en legitimiteitsassumpties in theorie	Manifestatie in ANPR-beleid Politie Nodaalstad
Controleperspectief	
Wijdverspreide controle van burgers	<ul style="list-style-type: none"> • ANPR kan zorgen voor beheersing. • Door ANPR kunnen criminelen niet ongezien de regiogrenzen overschrijden (ring of steel). • Met ANPR kan de politie de bewegingen van een geselecteerd voertuig reconstrueren. • ANPR kan helpen om verdachte voertuigen te selecteren uit vervoersstromen. • ANPR draagt bij aan nodale oriëntatie, en daarmee beheersing van de belangrijke knooppunten en stromen in de regio. • Aan de hand van ANPR-hotlists kan de politie mensen uit vervoersstromen selecteren.
Disciplineren van burgers	Niet aanwezig
Inzet van surveillance ten aanzien van burgers	<ul style="list-style-type: none"> • De politie mag ANPR gebruiken, omdat het de uitvoering van de politietask betreft. (legaliteit) • De politie mag ANPR-hotlists gebruiken om mensen uit vervoersstromen te selecteren. (legaliteit) • De politie mag op grond van de Wet Politiegegevens ANPR-analyses uitvoeren ten aanzien van concrete criminaliteitsproblemen. (legaliteit) • De Politie Nodaalstad mag zelf richtlijnen opstellen voor de omgang met gegevens op basis van een eigen interpretatie van wetgeving. (legaliteit) • De politie mag ANPR gebruiken in de opsporing op grond van jurisprudentie. (legaliteit) • De politie is genoodzaakt ANPR te gebruiken om de politietask nog te kunnen uitvoeren in de veranderde samenleving. (normatieve rechtvaardiging) • Het bewaren van ANPR-gegevens is nodig voor de moderne criminaliteitsbestrijding. (normatieve rechtvaardiging) • De politie moet ANPR inzetten om veiligheid in de veranderende samenleving te kunnen waarborgen. (normatieve rechtvaardiging) • ANPR is goed, omdat het de politie efficiënter en effectiever maakt. (normatieve rechtvaardiging) • ANPR is goed, omdat het nodale oriëntatie is. (normatieve rechtvaardiging) • ANPR is legitiem op grond van kenbaarheid van enkele kenmerken van het systeem (maatschappelijke acceptatie)

Technologie- en legitimiteitsassumpties in theorie		Manifestatie in ANPR-beleid Politie Nodaalstad
Controleperspectief		
Beschermen van privacy van burgers		<ul style="list-style-type: none"> De Politie Nodaalstad mag ANPR-gegevens inwinnen, omdat er sprake is van uitvoering van de politietaak bij een geringe inbreuk op de privacy. (legaliteit) De politie heeft een juridische grondslag nodig voor het bewaren van ANPR-gegevens. (legaliteit) De Politie Nodaalstad mag in het kader van veiligheid de privacy van burgers schenden. (maatschappelijke acceptatie)
Interactieperspectief		
Verbinden van overheid en burgers	Niet aanwezig	
Gezamenlijke informatiecreatie	Niet aanwezig	
Toegang tot surveillance-informatie		<ul style="list-style-type: none"> Voor toegang tot ANPR-gegevens van gemeentecamera's is bestuurlijke toestemming nodig. (maatschappelijke acceptatie)
Relevantie en kwaliteit van surveillance-informatie		<ul style="list-style-type: none"> De Politie Nodaalstad mag no-hits analyseren op grond van de Wet Politiegegevens. (legaliteit)
Voorzorgperspectief		
Identificeren van risico's en risicoburgers		<ul style="list-style-type: none"> ANPR draagt bij aan nodale oriëntatie, en daarmee het zichtbaar maken van risico's.
Beteugelen van risico's		<ul style="list-style-type: none"> De politie kan ANPR gebruiken om burgers die een risico vormen te selecteren. ANPR draagt bij aan nodale oriëntatie, en daarmee preventie van criminaliteit. De politie kan ANPR gebruiken om potentiële criminelen nader te onderzoeken De politie kan ANPR gebruiken om criminelen tegen te houden. ANPR verhoogt de pakkans van criminelen en overtredders
Definiëring van risico's en risicocategorieën burgers		<ul style="list-style-type: none"> Er zijn grenzen aan de categorieën burgers waar de politie de privacy van mag schenden met ANPR. (normatieve rechtvaardiging) Het is goed dat de politie ANPR inzet, omdat ze hierdoor efficiënter werkt met minder overlast voor onschuldige / onverdachte burgers. (normatieve rechtvaardiging) De Politie Nodaalstad moet ANPR proactief inzetten om de politietaak signalering en advisering te kunnen vervullen. (maatschappelijke acceptatie)

Tabel 10: Surveillanceperspectieven in het ANPR-beleid van de Politie Nodaalstad

Eén technologieassumptie is niet toe te schrijven aan een theoretisch surveillance-perspectief:

- ANPR heeft een nog nader te bepalen nut voor de politie.

Deze beleidsveronderstelling heeft vooral invloed op de beginfase van het ANPR-beleid. Het is dan ook niet verwonderlijk dat de politie op dat moment nog geen duidelijk perspectief heeft op surveillance.

4.3 Implicaties van het Nodaalse ANPR-beleid voor de relatie overheid-burger

De analyse laat zien dat het ANPR-beleid van de Politie Nodaalstad kenmerken vertoont van alle drie de surveillanceperspectieven. Met name het controleperspectief en het voorzorgperspectief helpen om de beleidsontwikkeling over ANPR te begrijpen. Het interactieperspectief drukt minder sterk een stempel op de beeldsvorming. Wat betekent dit ANPR-beleid nu voor de relatie tussen de Politie Nodaalstad en burgers? In hoofdstuk 4 heb ik de theoretische implicaties van de verschillende surveillanceperspectieven voor de relatie overheid-burger uiteengezet. Deze theoretische verwachtingen vertaal ik hier naar de empirie van de casus.

4.3.1 Implicaties van het Nodaalse ANPR-beleid voor de verhouding machthebber-onderdaan

CONTROLEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Surveillance faciliteert en vervangt overheidshandhaving van regelgeving.	ANPR faciliteert de verkeershandhaving van de politie door burgers die regels hebben overtreden te signaleren in het verkeer. Deze signaalfunctie wordt steeds sterker doordat er meer en uitgebreidere hotlists worden toegevoegd aan het systeem. Een gevolg is dat een (goed of slecht) voorgevoel van een politiefunctionaris niet langer een rol speelt bij het besluit tot staandehouding. De in het ANPR-systeem vermelde antecedenten bepalen of een voertuig in aanmerking komt voor verdere afhandeling. De daadwerkelijke afhandeling is wel volledig in handen van de politie. Er zijn vooralsnog geen aanwijzingen dat het ANPR-systeem meer vervangt dan de signaalfunctie van politiemensen. Zo instigeert het systeem geen automatische administratieve afhandeling, stopbericht aan de overtredende bestuurder of afstandscontrole over het voertuig.
Panoptische disciplineren zorgt ervoor dat burgers overheidsregels naleven.	De politie Nodaalstad zet niet bewust in op disciplineren van burgers, maar het is niet gezegd dat het ANPR-beleid geen disciplinerend effect kan hebben. Het korps maakt de aanwezigheid van het systeem immers kenbaar aan burgers via borden bij de camera's en uitspraken in de media. Over het precieze aantal hotlists en de aard hiervan voert de politie geen heldere communicatie. Hierdoor zijn burgers beperkt op de hoogte van de normen waarop de politie hen mogelijk controleert. Ze weten echter wel dat ze worden bekeken, waardoor het systeem alsnog een disciplinerende werking kan hebben.

INTERACTIEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Overheidsregelgeving en -handhaving worden aangevuld door burgernormen en -handhaving.	Hier is geen sprake van. Burgers hebben geen enkele invloed op de vaststelling van de normen waarop zij worden gecontroleerd door de politie. Ook zijn burgers niet in staat om een rol te spelen in de handhaving van medeburgers, aangezien zij geen toegang hebben tot de informatie in het ANPR-systeem. Andere partijen, zoals de Belastingdienst en de Douane leveren wel informatie aan voor het ANPR-systeem. Op basis van de informatie van deze overheidspartijen ontwikkelt de politie nieuwe hotlists en verbreedt ze haar handhavingstaak door burgers uit de verkeersstroom te halen die normen van deze andere overheidspartijen hebben overtreden.
Overheid en burgers stimuleren medeburgers om mee te werken aan handhaving.	Uit het ANPR-beleid spreekt geen enkele intentie om burgers te betrekken bij de handhaving van medeburgers. Er is bijvoorbeeld geen koppeling (voorzien) tussen het ANPR-systeem en Burgernet.
VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Overheidsregelgeving en -handhaving veranderen snel en richten zich op risicogroepen.	De politie richt zich er steeds meer op om naleving van regels te garanderen door te voorkomen dat burgers ze overtreden. Hierbij richt de politie zich op bekende criminelen en overtreeders, die al op één of meerdere hotlists voorkomen om deze groepen vervolgens aan te merken als potentiële criminelen en overtreeders wiens voertuigbewegingen aan nader onderzoek dienen te worden onderworpen. Er zijn geen aanwijzingen dat de politie in het ANPR-beleid risicogroepen definieert op basis van andere kenmerken dan bekendheid bij de politie.

VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Burgers verkeren in Kafkaëske onzekerheid door beperkte kennis over veranderlijke normen.	Ondanks dat de politie het ANPR-systeem (nog) niet gebruikt voor het identificeren van nog onbekende risico's, verkeren burgers wel in onzekerheid over de normen waarop ze gecontroleerd worden. Het is voor burgers tot op het moment van een eventuele aanhouding namelijk allerm minst inzichtelijk welke hotlists de politie precies hanteert en op basis van welke criteria deze worden samengesteld. Bovendien komen er in een rap tempo meer hotlists bij, waarover burgers niet worden geïnformeerd. Ook kan iemand die toch al in het vizier is als risicoburger, omdat hij op een bepaalde hotlist staat, worden verrast door de manier waarop de politie zijn voertuigpassages analyseert en daar acties aan koppelt.

Tabel 11: Implicaties van het Nodaalse ANPR-beleid voor de verhouding machthebber-onderdaan

4.3.2 Implicaties van het Nodaalse ANPR-beleid voor de verhouding dienstverlener-cliënt

CONTROLEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
De overheid verleent toegang tot en gemak bij publieke dienstverlening op basis van surveillancegegevens over burgers.	De politie ziet het gebruik van het ANPR-systeem als een service aan burgers die geen antecedenten hebben, omdat zij met rust worden gelaten. Deze burgers staan immers op geen enkele hotlist, waardoor het ANPR-systeem geen signaal zal geven als deze personen langs een cameralocatie rijden. De logica dat dankzij het ANPR-systeem onschuldige burgers niet worden lastiggevallen gebruikt de politie voorts als legitimatie

	<p>voor interventies op basis van de gegevens uit het ANPR-systeem. Ook is de politie zich ervan bewust dat de burgers die als cliënt worden onthaald efficiënter worden bediend, omdat hun gegevens al grotendeels bekend zijn op het moment van staandehouding.</p>
<p>Alle burgers worden reactieve of passieve cliënten.</p>	<p>Voorts worden burgers passieve cliënten van de veiligheidsdienstverlening van de politie in die zin dat een groot deel hiervan aan hen voorbijgaat. Ze merken er weinig van dat gegevens over voertuigpassages worden ingewonnen en opgeslagen, terwijl de samenleving er wel veiliger op wordt, zo is de bedoeling van het ANPR-beleid. Burgers worden reactieve cliënten op het moment dat hun voertuig gekoppeld wordt aan een overtreding of misdrijf (als verdachte, betrokkene of aandachtsvestiging) en ze door de politie om medewerking worden gevraagd.</p>
<p>INTERACTIEPERSPECTIEF</p>	
<p><i>Theoretische verwachtingen</i></p>	<p><i>Empirische bevindingen</i></p>
<p>De overheid wordt een passieve, modererende en reagerende dienstverlener.</p>	<p>Uit het ANPR-beleid spreekt de ambitie om steeds meer een proactieve dienstverlener te zijn die op basis van de nodale oriëntatie criminelen tegenhoudt. Tegelijkertijd zit de politie bij de directe opvolging sterk in de rol van reagerende dienstverlener, die handelt naar aanleiding van een voertuigpassage. Van een passieve of modererende rol van de politie is geen sprake.</p>
<p>Burgers vervangen door prosumptie van surveillance-informatie voor een groot deel de overheidsdienstverlening.</p>	<p>Doordat burgers geen toegang hebben tot elkaars ANPR-gegevens zijn ze niet in staat om de politie te helpen in haar dienstverlening of deze over te nemen. Het is bijvoorbeeld (nog) niet mogelijk voor een oplettende burger om wijkgenoten een bericht te sturen dat ze hun kinderen moeten binnenhouden, omdat een bekende pedofiel langs een cameralocatie aan het begin van de wijk is gereden.</p>

VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
<p>De overheid biedt dienstverlening selectief en proactief aan afhankelijk van groepskenmerken.</p> <p>Bepaalde groepen burgers worden reactieve of passieve cliënten.</p>	<p>In de benadering van haar cliënten, de burgers die de overheid een veilige samenleving en bescherming tegen onheil aanbiedt, maakt de politie in het ANPR-beleid geen onderscheid op basis van groepskenmerken. ANPR is weliswaar steeds meer gericht op het tegenhouden van potentiële daders, maar niet op het beschermen van potentiële slachtoffers. Er is echter één uitzondering: de inzet van ANPR-camera's voor de beveiliging van een prominent politicus. De politie Nodaalstad merkt deze toepassing zelf aan als een uitzondering, waar in de verdere beleidsontwikkeling geen speciale aandacht voor bestaat.</p>

Tabel 12: Implicaties van het Nodaalse ANPR-beleid voor de verhouding dienstverlener-cliënt

4.3.3 Implicaties van het Nodaalse ANPR-beleid voor de verhouding democratisch instituut-citoyen

CONTROLEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
<p>Door sousveillance maken burgers overheidssurveillance transparant.</p>	<p>De Politie Nodaalstad anticipeert in haar ANPR-beleid niet zozeer op burgers die het Nodaalse ANPR-systeem transparant proberen te maken, maar wel op allerlei maatschappelijke organisaties die hier belangstelling voor hebben. Het gaat dan om het CBP, maar ook wetenschappelijke instituten, zoals het Rathenau. Daarnaast merkt het korps dat andere politiekorpsen graag meer inzicht willen in het Nodaalse ANPR-beleid.</p>

Sousveillance zet de overheid aan tot verantwoording over de surveillance van burgers.	De aandacht van maatschappelijke spelers voor het Nodaalse ANPR-beleid en de kritiek die ze hier mogelijk op gaan leveren, geven het korps een extra zetje om de legitimiteit van haar beleid te onderzoeken en intern te verantwoorden, zodat het voorbereid is om desgevraagd tot publieke verantwoording over te gaan.
INTERACTIEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Surveillance faciliteert zelfsturing en coöperatie met de overheid.	Het ANPR-beleid geeft burgers geen middelen in handen om tot zelfsturing of coöperatie met de politie te komen. Een dergelijke actieve citizenrol wordt niet gestimuleerd.
Burgers eisen een actieve rol op in de handhaving van medeburgers.	Uit het ANPR-beleid volgen geen aanwijzingen dat burgers op deze manier invulling gaan geven aan hun citizenrol.
VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Risicoanalyses staan centraal in de verantwoording van beleidskeuzes.	Het korps treedt nog weinig naar buiten over de eerste proactieve toepassingen van ANPR. Op basis van de ANPR-beleidsontwikkeling en de door het korps gewenste profilering als innovator valt wel te verwachten dat de politie haar aanpak van risicogroepen zal verantwoorden door te wijzen op het gebruik van innovatieve technologie, mits de juridisch-maatschappelijke discussie is uitgekristalliseerd.
Risico's op de publieke agenda bereiken gemakkelijk de surveillanceagenda van de overheid.	Uit het ANPR-beleid volgen geen aanwijzingen dat het publiek invloed heeft op de selectie van risico's die de politie wil gaan beteugelen met ANPR. Deze keuze ligt bij de korpsleiding en bij de uitvoering binnen de LAD.

Tabel 13: Implicaties van het Nodaalse ANPR-beleid voor de verhouding democratisch instituut-citoyen

5 Conclusie

In het ANPR-beleid van de Politie Nodaalstad zijn met name het controleperspectief en het voorzorgperspectief op surveillance te zien. Voor de verhouding machthebber-onderdaan betekent dit dat de traditionele signaalfunctie van de politie bij de handhaving van regelgeving grotendeels wordt overgenomen door het ANPR-systeem en dat de politie zich in toenemende mate richt op het tegenhouden van misdrijven en overtredingen door risicogroepen. In de benadering van cliënten hanteert de dienstverlenende politie meer een controleperspectief dan een voorzorgperspectief. Met de inzet van ANPR wil de politie alle burgers in gelijke mate een veilige samenleving garanderen en wijst ze, op een politieke prominent na, geen groepen burgers aan die wellicht bescherming op maat kunnen gebruiken. Daarbij ziet de politie het gebruik van het ANPR-systeem als een service aan burgers die geen antecedenten hebben, omdat zij met rust worden gelaten, en legitimeert het systeem ook als zodanig. De invulling van de verhouding democratisch instituut-citoyen wordt bepaald door de dreiging van sousveillance en de bijbehorende mogelijkheid van maatschappelijke en juridische afkeuring van het ANPR-beleid. Om die reden tast het korps de maatschappelijke acceptatie van met name de proactieve toepassing van ANPR af en investeert het in het opstellen van een juridisch kader. Tegelijkertijd staat de Nodaalse politie klaar om de innovatieve aanpak van bepaalde groepen criminelen wereldkundig te maken.

Epiloog

De hoopvolle stemming waarin ik het politiekorps Nodaalstad in 2009 verlaat, loopt begin 2010 een flinke deuk op wanneer het College Bescherming Persoonsgegevens concludeert dat een aantal politiekorpsen willens en wetens de wet overtreden door no-hits te bewaren (College Bescherming Persoonsgegevens, 2010). De opdracht van het CBP om alle no-hitgegevens uit politiebestanden te verwijderen, geldt vervolgens ook voor de Politie Nodaalstad. Zo wordt duidelijk wat legitiem is, maar vooral wat niet legitiem is qua ANPR-toepassingen. De terechtwijzing van het CBP is een belangrijke indicatie dat het noch maatschappelijk, noch wettelijk acceptabel is om no-hits op te slaan. De gedane investeringen in ANPR-apparatuur, organisatorische ondersteuning en contacten met andere korpsen, de landelijke politieorganisatie en de voormalige ministeries van BZK en Justitie betalen zich wel uit in gegroeide politieke steun voor de doorontwikkeling van ANPR. In het regeerakkoord van het kabinet-Rutte-Verhagen is te lezen: 'Voertuigherkenning draagt bij aan preventie en vereenvoudiging van opsporing en vervolging van strafbare feiten en aan de handhaving van fiscale verplichtingen. Hiertoe komt er een bredere inzet van systemen van automatische

nummerplaatherkenning' (Rijksoverheid, 2010: 42). Op 12 februari 2013 resulteert dit voornemen in de presentatie van een wetsvoorstel aan de Tweede Kamer:

‘Minister Opstelten van Veiligheid en Justitie heeft een wetsvoorstel bij de Tweede Kamer ingediend waardoor alle kentekens die de politie met camera’s automatisch vastlegt, vier weken mogen worden bewaard om misdrijven op te sporen en voortvluchtige verdachten en veroordeelden aan te houden.’

(Rijksoverheid, 2013b)

HOOFDSTUK 7

INNOVATIE BIJ DE INWINNING EN VERWERKING VAN VERKEERSGEGEVENS

1 Inleiding

Innovatie is wat de Nationale Databank Wegverkeersgegevens (NDW) voor ogen heeft als ze in het najaar van 2009 start met de voorbereidingen van een aanbesteding voor de inwinning en verwerking van verkeersgegevens in de regio Noord- en Oost-Nederland (NON). Welke technologieën precies gebruikt moeten gaan worden om gegevens over de activiteit op de wegen in NON te verzamelen, weet NDW op dat moment nog niet. Wel anticipeert ze erop dat floating-car-data de gewenste innovatie zouden kunnen bewerkstelligen. In tegenstelling tot het gebruikelijke inwinsysteem van lussen in de weg en vaste camera's op de weg, verzamelt een floating-car-datasysteem gegevens uit voertuigen zelf. Een belangrijk kenmerk van dit type innovatieve systemen is de beschikbaarheid van actuele mobiliteitsgegevens over een voertuig. Dit kan gaan om de voertuigcategorie, de snelheid en ook de actuele locatie. Zodoende zijn dergelijke innovatieve verkeerssystemen te beschouwen als een manifestatie van publieke mobiliteitssurveillance. Ten tijde van het casusonderzoek, dat plaatsvindt van december 2009 tot en met oktober 2010, is het realiseren van innovatie in de inwinning en verwerking van verkeersgegevens een belangrijk beleidsdoel van NDW. De zoektocht naar innovatie krijgt gestalte in de voorbereiding en uitvoering van de aanbesteding voor de regio NON.

In dit hoofdstuk analyseer ik in hoeverre de surveillanceperspectieven controle, interactie en voorzorg aanwezig zijn in het innovatiebeleid van NDW ten aanzien van de inwinning en verwerking van verkeersgegevens en welke implicaties voor de relatie overheid-burger hieraan verbonden zijn.

Eerst geef ik een toelichting op de organisatie NDW en hoe deze in de aanloop naar de aanbesteding NON begint met het verkennen van innovatie als nieuw beleidsthema. Vervolgens beschrijf ik hoe het innovatiebeleid verder wordt uitgewerkt in de aanbesteding voor NON. Hierbij ga ik achtereenvolgens in op drie fases in het aanbestedingsproces: het formuleren van de aanbestedingsvraag, een marktconsultatie, en tenslotte de fase van publicatie, beoordeling en gunning. Bepalend voor de beleidsontwikkeling rondom innovatie zijn de veronderstellingen die NDW erop nahoudt over de functie van innovatieve technologie in het verkeersdomein (technologieassumpties) en over de gronden waarop innovatieve technologie wordt toegepast (legitimiteitsassumpties).

Evenals in hoofdstuk 6 plaats ik door de casusbeschrijving heen tekstballonnen met door mij aangetroffen technologie- en legitimiteitsassumpties bij passages die illustratief zijn voor de betreffende assumpties.⁵⁶

In de daaropvolgende paragraaf volgt de analyse van het innovatiebeleid van NDW. In de analyse vat ik ten eerste samen welke technologie- en legitimiteitsassumpties uit het innovatiebeleid spreken. Als tweede stap van de analyse verbind ik de aangetroffen technologie- en legitimiteitsassumpties aan de assumpties die ik in hoofdstuk 4 per theoretisch surveillanceperspectief heb vastgesteld. Zo wordt inzichtelijk in hoeverre NDW in het innovatiebeleid een controle-, interactie- of voorzorgperspectief op surveillance laat zien. Als derde en laatste analysestap ga ik in op wat de surveillanceperspectieven die zijn aangetroffen in het beleid betekenen voor de relatie overheid-burger. Hierbij bespreek ik op welke punten de theoretisch verwachte invulling van de verhoudingen machthebber-onderdaan, dienstverlener-cliënt en democratisch instituut-citoyen empirische werkelijkheid wordt. Zodoende ontstaat een empirische inkleuring van het theoretisch kader dat ik aan het eind van hoofdstuk 4 heb gepresenteerd.

2 NDW en de aanloop naar de aanbesteding NON

2.1 De Nationale Databank Wegverkeersgegevens

Na een voorbereidingsfase van 2006 tot en met 2008 wordt op 6 juli 2009 de Nationale Databank Wegverkeersgegevens (NDW) officieel geopend door de toenmalige minister van Verkeer en Waterstaat Camiel Eurlings. De aanduiding NDW staat niet alleen voor het technische systeem waarmee wegverkeersgegevens worden beheerd, maar ook voor de organisatie hieromheen. De missie van NDW luidt:

‘NDW draagt als netwerkorganisatie bij aan de mobiliteit in Nederland door te voorzien in een betrouwbare, toekomstgerichte en kostenefficiënte landelijke informatiehuishouding voor het verwerven, opslaan, beheren en beschikbaar stellen van voor wegverkeer relevante gegevens en door het stimuleren van het gebruik daarvan.’

(Ondernemingsplan NDW 2008-2013)

⁵⁶ Het gaat hierbij om technologie- en legitimiteitsassumpties van het NDW-innovatiebeleid en niet van mijzelf.

Deze missie vloeit voort uit de Nota Mobiliteit uit 2004 van het toenmalige Ministerie van Verkeer en Waterstaat, waarin oplossingsrichtingen zijn geformuleerd voor het garanderen van een goede bereikbaarheid binnen Nederland.⁵⁷ NDW wil zich graag profileren als netwerkorganisatie van publieke en private partijen die betrokken zijn bij verkeersmanagement en het leveren van verkeersinformatie in Nederland. Verkeersmanagement en verkeersinformatie zijn sterk met elkaar verbonden. Het publiek voorzien van verkeersinformatie is een manier om het gebruik van het wegennet te sturen en als zodanig een belangrijk uitvoeringsinstrument voor verkeersmanagement. In het geval van een file geven dynamische verkeersinformatiepanelen (DRIPs) bijvoorbeeld suggesties voor een alternatieve route om te voorkomen dat de file veel langer wordt. Andersom is inzicht in de toestand op de wegen essentieel voor het opstellen van adequate verkeersinformatie. Om automobilisten te kunnen waarschuwen voor zaken als wegversperringen, ongelukken en files moeten wegbeheerders en andere producenten van verkeersinformatie hiervan tijdig op de hoogte zijn. Het inwinnen van wegverkeersgegevens ligt aan de basis van zowel het verkeersmanagement door wegbeheerders als het verstrekken van verkeersinformatie door private partijen. Volgens NDW gebeurt dit in 2008 versnipperd en incompleet:

‘Het Rijk, de provincies, regio’s en de gemeenten hebben allemaal hun eigen, of helemaal geen informatiesystemen. Dat is een probleem voor zowel weggebruikers als wegbeheerders.’

(Ondernemingsplan NDW 2008-2013)

Verschillende NDW’ers geven aan dat NDW met name een centrale, coördinerende rol wil vervullen in de keten van organisaties die gezamenlijk zorg dragen voor verkeersmanagement en verkeersinformatie. Naast het uitvoerende werk, bestaande uit het opbouwen en beheren van de database met wegverkeersgegevens, ziet NDW ook een rol voor zich weggelegd bij nieuwe beleidsvorming. NDW houdt ontwikkelingen in de technologiemarkt en in de beleidsvorming bij de overheidspartners in de gaten en signaleert waar nieuwe kansen en risico’s zich voordoen op het gebied van wegverkeersgegevens. Stafmedewerkers vertellen over de behandeling van de nota ‘multimodale reisinformatie’ in de Tweede Kamer, waarin voor NDW een specifieke taak is weggelegd voor het aanleveren van gegevens van de weg.⁵⁸

Hoewel NDW formeel gezien een publieke uitvoeringsorganisatie is, is deze betiteling volgens de NDW’ers die ik spreek minder van toepassing, omdat deze slechts een deel van het werk van NDW beslaat. Ook al heeft NDW een eigen directie, staf,

⁵⁷ Voor een beschrijving van de beleidscontext waarin de oprichting van NDW heeft plaatsgevonden, zie het proefschrift van Bonno Pel (2012)

⁵⁸ Andere organisaties leveren gegevens over het openbaar vervoer.

beleidsadviseur en operationele medewerkers (12,5 fte in totaal), ze wordt niet opgericht als zelfstandige juridische entiteit, maar valt onder Rijkswaterstaat (RWS) binnen het toenmalige Ministerie van Verkeer en Waterstaat. Rijkswaterstaat treedt op ‘als gastheer voor de uitvoeringsorganisatie, die daar als losstaand onderdeel wordt gefaciliteerd’, zo vermeldt het ondernemingsplan van NDW. In de praktijk betekent dit dat Rijkswaterstaat zorg draagt voor zaken als huisvesting en ICT-infrastructuur voor de medewerkers. De directeur van NDW heeft zelfstandige tekenbevoegdheid. De NDW-directie rapporteert aan een Raad van Toezicht. Deze Raad van Toezicht bestaat uit bestuurders die de vier groepen overheidsorganisaties die NDW financieren vertegenwoordigen: Rijkswaterstaat, provinciale wegbeheerders, gemeentelijke wegbeheerders en (stads)regio’s. ‘*Wij zijn van alle wegbeheerders*’, zo verklaart een NDW-beleidsmedewerker. Het jaarplan van NDW wordt opgesteld samen met alle aangesloten overheidsorganisaties, ook wel partners genoemd. Bij de start van NDW gaat het om vijftien overheden, die binnen NDW de koplopers worden genoemd, omdat zij betrokken zijn bij de oprichting van NDW en de eerste partners zijn. De koplopersgroep wordt gevormd door Rijkswaterstaat, de gemeenten Amsterdam, Rotterdam, Den Haag en Utrecht, de provincies Noord-Brabant, Noord-Holland, Utrecht en Zuid-Holland, de regio Utrecht en de stadsregio’s Amsterdam, Arnhem-Nijmegen, Eindhoven en Rotterdam en het stadsgewest Haaglanden (Ondernemingsplan NDW 2008-2013). De hoogte van financiële bijdrage van iedere partner hangt af van het aantal gegevens dat ze ‘inbrengen in NDW’. Zodoende is Rijkswaterstaat verreweg de grootste partner, omdat deze partij alle autosnelwegen in haar beheer heeft.

Bij de start van NDW zijn het de wegen op de grondgebieden van deze vijftien koplopers waarover NDW wegverkeersgegevens dient te verzamelen, verwerken en beschikbaar stellen aan haar afnemers. NDW heeft dus nog geen overeenkomst met alle wegbeheerders in Nederland. Die overheden winnen op dat moment zelf wegverkeersgegevens in of doen dat nog helemaal niet. Op termijn wil NDW haar netwerk uitbreiden tot ‘alle relevante doorgaande wegen in Nederland (zo’n 10.000 kilometer)’ (Folder NDW uitgelegd). NDW maakt betreffende de gegevens die ze verwerkt een onderscheid tussen statusgegevens en verkeersgegevens. NDW beschrijft statusgegevens als ‘beschikbaarheid van de weg’, waarbij het gaat om informatie over zaken als wegwerkzaamheden, bruggen en spitsstroken. Verkeersgegevens zijn kenmerken van een verkeersstroom op een locatie en hebben zodoende betrekking op de ‘beschikbaarheid op de weg’. NDW onderscheidt vijf typen verkeersgegevens: verkeersintensiteit, gerealiseerde reistijd, geschatte reistijd, puntsnelheden en voertuigcategorieën. De reikwijdte van NDW is in het najaar van 2009 zowel in geografisch opzicht als qua gegevenstypen en -kwaliteit nog vrij beperkt.

Hoe komt NDW aan de gewenste status- en verkeersgegevens en waar gaan ze naartoe? Deze worden aangeleverd door interne en externe dataproviders. Interne dataproviders zijn bij NDW aangesloten wegbeheerders⁵⁹ die ervoor kiezen om zelf wegverkeersgegevens in te (laten) winnen en aan te leveren aan NDW. Hierbij zijn zij, evenals de externe dataproviders gebonden aan de door NDW opgestelde kwaliteitseisen aan de data. Dit zijn gekwantificeerde eisen betreffende de nauwkeurigheid, beschikbaarheid, betrouwbaarheid en actualiteit van de gegevens. NDW-partners kunnen er ook voor kiezen om wegverkeersgegevens niet zelf in te winnen, maar dit voor een deel of het geheel van hun wegen over te laten aan partijen die worden ingehuurd door NDW. In dat geval spreekt men van externe dataproviders. Na ontvangst van actuele wegverkeersgegevens van interne en externe dataproviders stuurt NDW deze door naar haar afnemers en zorgt voor de aanleg van een bestand van historische wegverkeersgegevens. De afnemers van NDW zijn enerzijds de aangesloten wegbeheerders, waarvan sommigen als interne dataproviders hun eigen gegevens terugkrijgen en anderzijds leveranciers van verkeersinformatie aan weggebruikers. NDW is zodoende een indirecte informatieleverancier aan burgers. NDW heeft weinig tot geen direct contact met individuele burgers. De oprichting van NDW is al wel in het nieuws geweest, NDW heeft een publieke website, maar biedt geen directe diensten aan burgers.

Bij haar officiële start medio 2009 heeft ze echter nog veel werk te verrichten om de netwerkorganisatie voor wegverkeersgegevens te worden. Hiervoor heeft ze een goed gevulde database nodig, die zowel afhangt van het aantal aangesloten overheidspartners als van de realisatie van de gegevensinwinning door dataproviders. Daarnaast is het voor haar positie in de verkeersmarkt belangrijk om nieuwe afnemers te vinden.

Om de gewenste uitbreiding te realiseren en de politiek-bestuurlijke steun voor NDW te continueren, start NDW in het najaar van 2009 de voorbereidingen voor de Europese aanbesteding van de inwinning van verkeersgegevens voor het geografische perceel Noord- en Oost-Nederland (NON). Eerder heeft ze via een aanbesteding voor de percelen Randstad en Zuid-Nederland een externe dataprovider gecontracteerd. Het verloop en de uitkomst van deze eerdere aanbesteding laat zijn sporen na in het innovatiebeleid van NDW en de daarbij horende aanbesteding NON. Ook zijn er beleidsontwikkelingen in het voorjaar van 2009 die van invloed blijken te zijn op de aanbesteding NON.

⁵⁹ Hierbij worden vijf categorieën onderscheiden: stedelijke, regionale en provinciale verkeerscentrales, wegbeheerders zonder verkeerscentrales en samenwerkingsverbanden van overheden (Rijkswaterstaat: Eisen aan de Nationale Databank Wegverkeersgegevens (NDW) systeemketen 12-12-2008).

2.2 Aanloop naar de aanbesteding NON

Vanaf medio 2008 gaat de eerste aanbesteding voor de inwinning en verwerking van verkeersgegevens ten behoeve van NDW van start. Op dat moment is NDW nog geen zelfstandige uitvoeringsorganisatie, maar een project binnen RWS. Zodoende is het Rijkswaterstaat die optreedt als opdrachtgever voor de aanbesteding en de RWS Data-ICT dienst die het aanbestedingstraject formeel voor NDW uitvoert. In de opdrachtschrijving wordt duidelijk gespecificeerd dat het gaat om gegevensinwinning ten behoeve van de nog op te richten NDW. Het is de intentie van de aanbesteding om in één keer externe dataproviders aan te trekken voor het gehele Nederlandse basiswegennet, bestaande uit zo'n 5000 kilometer aan autosnelwegen, provinciale en stedelijke wegen.⁶⁰ Op 12 december 2008 wordt de opdracht grotendeels gegund aan het consortium ARA, bestaande uit verkeers- en transporttechnologiebedrijf ARS en ingenieursorganisatie Arcadis. Op de website van NDW wordt het volgende nieuwsbericht gepubliceerd:

‘Vandaag ondertekenden ARA en de Nationale Databank Wegverkeersgegevens (NDW) het contract voor de inwinning van actuele verkeersgegevens in de Randstad en Zuid-Nederland voor NDW. Door middel van camera's en lussen in het asfalt zal ARA gegevens over de doorstroming en snelheid van verkeer op de belangrijkste doorgaande wegen in die gebieden gaan meten.’

Omdat het consortium ARA als enige van de drie aanbiedende partijen kan voldoen aan de kwaliteitseisen van NDW gaat ARA voor twee van de drie geografische percelen de inwinning van verkeersgegevens verzorgen. Het derde geografische perceel, Noord- en Oost-Nederland wordt in deze aanbesteding uiteindelijk niet gegund. Een consultant die betrokken was bij de opzet van deze eerste aanbesteding vertelt me dat RWS in het bestek had opgenomen om één aanbieder maximaal twee percelen te gunnen om zo de concurrentie op de markt te bevorderen. Hiermee komt het derde perceel te vervallen in de eerste aanbesteding en moet dit later opnieuw worden aanbesteed. De inmiddels op poten gezette NDW-organisatie grijpt in het najaar van 2009 de nieuwe aanbesteding van NON aan om innovatie te stimuleren. De combinatie van lustechniek en ANPR die ARA gebruikt voor de inwinning van verkeersgegevens in de Randstad en Zuid-Nederland beschouwt NDW als bewezen,

⁶⁰ De omvang en samenstelling van het volledige basisnetwerk, bestaande uit de wegen van de NDW-koplopers, staat gespecificeerd in Bijlage 10 van het Selectiedocument aanbesteding geografische percelen NDW d.d. 4 januari 2008.

maar traditioneel. NDW komt tot dit standpunt in de nabeschouwing van de eerste aanbesteding die ze in 2008 samen met marktpartijen houdt. Ook al weet NDW nog niet precies welke andere technieken marktpartijen te bieden hebben, ze is ervan overtuigd dat er innovatie in de markt zit en zou graag zien dat deze daadwerkelijk tot uiting komt ten behoeve van NDW. Het verlangen naar innovatie komt voort uit een combinatie van politiek-bestuurlijke druk en druk vanuit de markt. Zo hoor ik van de NDW-top dat de minister innovatie verlangt en verwacht. Deze lezing strookt met een observatie van onderzoeker Bonno Pel:

‘In accordance with his traffic management policy framework published only a few months earlier (Ministerie van Verkeer en Waterstaat, 2007), he [de minister – CvO] stressed the rise of in-car systems to be both inevitable and feasible. Adequate public-private agreements he indicated as the way to proceed.’

(Pel, 2012: 216)

De politiek-bestuurlijke druk groeit door de toenaderingen van een serviceprovider richting de Tweede Kamer. Als innovatieve speler op de verkeersmarkt stelt dit bedrijf, ‘serviceprovider X’,⁶¹ zich op als een concurrent van NDW. De serviceprovider wil politieke toestemming om zelf verkeersgegevens in te winnen en reisinformatie aan te bieden. Hierbij stelt het bedrijf veel goedkoper te zijn dan NDW. Door de lobbyactiviteiten van serviceprovider X voelt NDW een nog sterkere noodzaak om in Den Haag te laten zien dat zij wel degelijk innovatie kan bewerkstelligen en daarbij de hoogste kwaliteit verkeersgegevens kan leveren.

Legitimiteitsassumptie 1:

NDW moet innovatieve technologie inzetten, omdat dit politiek-bestuurlijk wordt verwacht. (maatschappelijke acceptatie)

NDW benadrukt het verschil in kwaliteitsbehoefte voor de verkeersinformatiemarkt en die van verkeersmanagement. Zo zijn floating-car-data, die serviceprovider X kan bieden wel geschikt voor het berekenen van reistijden, maar niet voor de bepaling van intensiteiten, die nodig zijn voor verkeersmanagementdoeleinden. NDW stelt hogere eisen aan de kwaliteit van de in te winnen verkeersgegevens, zodat deze ook gebruikt kunnen worden voor verkeersmanagementdoeleinden.

⁶¹ Namen van marktpartijen worden op verzoek van NDW geanonimiseerd.

In een stuurgroepvergadering tijdens het aanbestedingstraject laat NDW blijken in de lobbyende serviceprovider een potentiële leverancier van innovatieve technieken te zien: *‘Het mooiste is als serviceprovider X kan gaan aanbieden, want dan zijn we over een heleboel wazige discussies in de Tweede Kamer heen’*. Mocht de serviceprovider inderdaad gaan aanbieden en vervolgens de aanbesteding winnen dan zou het bedrijf opdrachtnemer worden van NDW en zo meestromen in NDW’s politieke vaarwater in plaats van ertegen ingaan.

Legitimiteitsassumptie 2:

Het is wenselijk dat innovatie geleverd wordt door serviceprovider X. (maatschappelijke acceptatie)

Naast de politiek-bestuurlijke druk ervaart NDW ook druk vanuit de verkeersmarkt om het gebruik van innovatieve inwintechneken mogelijk te maken. In een aanbestedingsvergadering wordt vanuit NDW gezegd:

‘Ik word gek van de markt die zegt: “NDW, jullie zijn ouderwets. Er is allang innovatie, zie serviceprovider X.” Ik wil nu voorkomen dat het niet lukt door onze wijze van aanbesteden.’

Legitimiteitsassumptie 3:

NDW moet innovatieve technologie inzetten ten behoeve van haar positie op de verkeersmarkt. (maatschappelijke acceptatie)

NDW kan het zich niet veroorloven om gezichtsverlies te lijden ten aanzien van haar partners in de markt. Dit kan NDW op twee manieren duur komen te staan. Enerzijds is er het risico dat innovatieve aanbieders geen tijd en moeite zullen willen investeren om zich in te schrijven op een aanbesteding van NDW, omdat zij de kans groot achten niet als winnaars uit de bus te komen. Anderzijds wil NDW het aantal afnemers van haar diensten op de private markt graag uitbreiden, maar die zullen minder geïnteresseerd zijn als er geen innovatie in het spel is. De druk van zowel publieke als private zijde wordt groter, omdat de eerste aanbesteding geen innovatie heeft opgeleverd. NDW heeft nog voordat ze officieel van start gaat sterk het gevoel zich te moeten bewijzen aan overheid en markt. Daarom stelt ze alles in het werk om mogelijke twijfel over de toegevoegde waarde van NDW voor het verkeersbeleid en de verkeersmarkt weg te nemen.

Legitimiteitsassumptie 4:

Innovatie is wenselijk voor het voortbestaan van NDW. (maatschappelijke acceptatie)

NDW's visie op innovatie komt in belangrijke mate tot stand naar aanleiding van twee bijeenkomsten met marktpartijen in de eerste helft van 2009. Op 3 maart 2009 vindt een 'inspiratiebijeenkomst met marktpartijen en een aantal experts'⁶² plaats, die wordt uitgewerkt in de beleidsnotitie 'Aanpak NDW regio Noord Oost. Innovatie, uitdaging voor ondernemers' van 29 mei 2009. Volgend op deze notitie houdt NDW op 8 juni 2009 een rondetafelgesprek met marktpartijen over 'de risico's en belemmeringen die samenhangen met het aanbieden van innovatieve inwintechnieken'.⁶³ Tijdens de inspiratiebijeenkomst presenteert hoogleraar Serge Hoogendoorn van de TU Delft zijn visie op de inwinning van verkeersgegevens. De kern van zijn betoog komt neer op een hybride aanpak met datafusie. In de beleidsnotitie wordt deze aanpak als volgt uitgelegd:

'Door het combineren van traditionele wegkantssystemen met innovatieve inwintechnieken, zoals bijvoorbeeld floating-car-systemen, kan volgens hem [Serge Hoogendoorn – toevoeging CvO] toch de voor NDW gewenste gegevenskwaliteit gerealiseerd worden.'

Hiermee maakt Hoogendoorn het concept innovatie concreter en tastbaarder voor NDW. Het liefst ziet hij datafusie plaatsvinden in een consortium van partners, met daarin opgenomen een leverancier van floating-car-data. Daarnaast lijkt datafusie voor NDW economisch aantrekkelijk te zijn. Ook heeft NDW van de aanwezige marktpartijen inzicht gekregen in de risico's en belemmeringen die samenhangen met de gewenste innovatie. In de rondetafelsessie wil NDW met marktpartijen mogelijkheden bespreken om deze 'zodanig beheersbaar te maken dat innovatie aantrekkelijk is voor de marktpartijen'.

Legitimiteitsassumptie 5:

Door de inzet van innovatieve inwintechnieken kan NDW verkeersgegevens goedkoper inwinnen. (normatieve rechtvaardiging)

Ook al stelt NDW dat 'de bijeenkomsten en de notitie op geen enkele wijze een onderdeel vormt van de komende aanbestedingsprocedure', worden de uitkomsten hiervan 'door het projectteam NDW meegenomen in de inhoudelijke uitwerking en procesmatige voorbereiding van de komende aanbestedingsprocedure voor de regio Noord Oost'. Op basis van de inspiratiesessie en het rondetafelgesprek formuleert

⁶² Omschrijving uit betreffende beleidsnotitie.

⁶³ Verslag rondetafelgesprek NDW en marktpartijen.

NDW een aantal maatregelen om innovatie te bevorderen. ‘Deze maatregelen kunnen onderdeel gaan vormen van de aanbestedingsdocumenten’, zo vermeldt het verslag van het rondetafelgesprek. Via vier paden kan innovatie worden gestimuleerd, zo luidt de voorlopige conclusie. Ten eerste kunnen de specificaties, technische eisen en de gunningscriteria in het bestek innovatie bevorderen. Het beperken van financiële en technische risico’s biedt een tweede en derde manier. Als laatste zou het beperken van de eisen goed zijn voor innovatie.

In een eerste gesprek met de directeur en een staflid van NDW in november 2009 krijg ik te horen dat het bestek voor de aanbesteding NON nog niet definitief is geformuleerd, maar dat hier de laatste hand aan wordt gelegd. Naar verwachting wordt de aanbesteding eind van dit jaar opengesteld, zo bevestigen beiden. Ondanks dat de directeur benadrukt dat zij zoeken naar innovatieve technieken, durven de twee echter niet te garanderen dat de uiteindelijke keuze niet zal vallen op bewezen technologie zoals lussen en camera’s. Volgens hen kleven er voor de marktpartijen aardig wat risico’s aan het aanbieden van innovatieve technieken. Deze hebben zich immers nog niet bewezen. De risicoverdeling tussen marktpartijen en NDW is een issue alsmede de kwaliteitseisen die NDW stelt aan de te leveren data. Zo wordt mij verteld dat een vertegenwoordiger van serviceprovider X in een gesprek met NDW aangaf terughoudend te zijn om samen met andere private partijen een consortium aan te gaan om de door NDW geëiste kwaliteit van verkeersgegevens voor het derde perceel te kunnen leveren. Het bedrijf zou wel bereid zijn om ingewonnen gegevens te verstrekken aan NDW, maar niet via NDW door te willen leveren aan andere private partijen (concurrenten). Tegelijk ziet het bedrijf ook een risico als het buiten de aanbesteding komt te vallen, omdat het dan niet de beschikking krijgt over de gegevens die de andere partijen verzamelen. Daarnaast hebben de serviceprovider en NDW gesproken over risico’s van een keuze voor in-car data. Het bedrijf noemt onder andere het probleem van de automobilist die altijd de apparatuur kan uitschakelen, waardoor geen gegevens vrij zouden komen. Verder is de penetratiegraad van de apparatuur een mogelijk probleem. Er moeten wel genoeg mensen zijn die de apparatuur in de auto hebben zitten.

Aan de kwaliteitseisen wordt onder geen beding getornd, zo vermeldt de beleidsnotitie over innovatie en hoor ik nogmaals in dit gesprek aan de vooravond van het aanbestedingstraject NON. Er bestaat op dat moment geen aanleiding om de kwaliteitseisen bij te stellen. In de loop van het aanbestedingsproces wordt echter duidelijk dat er wel degelijk aanpassingen nodig zijn. De aanbesteding wordt voorbereid en uitgevoerd door een projectteam dat ik gedurende het gehele proces volg. In december 2009 komt het projectteam voor het eerst bijeen.

3 Op zoek naar innovatie

3.1 Formuleren van de aanbestedingsvraag

3.1.1 Start van de projectgroep

Begin december 2009 sluit ik aan bij het eerste projectteamoverleg voor de aanbesteding NON. Het projectteam bestaat uit een extern ingehuurde aanbestedingsjurist, ondersteund door een projectsecretaris van hetzelfde bureau en één vertegenwoordiger van NDW, die formeel geen NDW-medewerker is, maar als zelfstandig consultant al jaren werkzaam is voor NDW en Rijkswaterstaat. NDW heeft ervoor gekozen om de aanbestedingsjurist tot projectleider te benoemen. *‘We gaan een planning maken en de uitgangspunten voor de aanbesteding op een rij zetten.’*, zo lees ik in een e-mail van één van de juristen.

Tijdens het drie uur durende overleg is het vooral de NDW-vertegenwoordiger die het woord neemt. In een uitgebreide presentatie zet hij de overwegingen voor de insteek van het aanbestedingsproces op een rijtje. Vanwege de omvang van de gevraagde dienst is de aanbesteding NON een Europese aanbesteding. Hiervoor gaat nu een openbare procedure plaatsvinden, die een aanzienlijk kortere doorlooptijd heeft dan een gesloten procedure, waarvoor gekozen was bij de vorige aanbesteding. Bij een openbare procedure zitten er maximaal 52 dagen tussen de aankondiging door de opdrachtgever en het indienen van inschrijvingen van potentiële opdrachtnemers. Met een vooruitziende blik wijst hij erop dat er een aandachtspunt is voor NDW nu er gekozen is voor een openbare procedure: *‘het bestek⁶⁴ moet compleet zijn bij de aankondiging’*. Voorts wordt duidelijk dat deze formele verantwoordelijkheid van opdrachtgever NDW afhangt van Rijkswaterstaat: *‘de kritische factor is RWS met het klaar hebben van de besteklijst’*. In dit bestek moet *‘een grotere rol voor innovatie’* komen door de gunningscriteria en wegingsfactoren te veranderen. Vervolgens wijst de NDW-vertegenwoordiger op een bijlage over innovatie in de Statement of Work (SOW) van de vorige aanbesteding. De SOW is één van de op te leveren aanbestedingsdocumenten en behelst een beschrijving van de

Legitimiteitsassumptie 6:

NDW mag innovatieve technologie alleen inzetten indien deze naar voren komt uit een Europese aanbestedingsprocedure. (legaliteit)

⁶⁴ Het bestek is de exacte omschrijving van de aanbestede opdracht.

omvang van de leveringen. Hij zal de SOW aanpassen aan de huidige aanbesteding en in het bijzonder kijken naar de innovatiebijlage. De jurist geeft mij na afloop van de vergadering echter aan dat ze wil gaan aansturen op de formulering van harde criteria, die gelden als geformaliseerde redenen voor innovatie in plaats van te werken met een innovatiebijlage. Tijdens de vergadering nemen de projectleden de redenen door waarom NDW überhaupt innovatie nastreeft. De NDW-medewerker noemt er vier:

- Door te investeren in innovatie bereidt NDW zich voor op de toekomst.
- NDW wil zo min mogelijk hinder bij aanleg van de meetapparatuur.
- NDW wil zo min mogelijk kastjes en palen langs de weg. Deze obstakels kunnen een risico zijn voor de veiligheid en vereisen extra maatregelen.
- Innovatieve technieken garanderen een gecontinueerde levering van gegevens bij wegwerkzaamheden.

Legitimiteitsassumptie 7:

Innovatieve technieken zijn wenselijk, omdat ze bijdragen aan de veiligheid van weggebruikers.
(normatieve rechtvaardiging)

Teruggrijpend op de inspiratiesessie en het rondetafelgesprek, waar de NDW-vertegenwoordiger zelf een actieve rol in heeft gehad, benadrukt hij dat de kwaliteit en de soorten gegevens vastliggen en dat innovatie alleen mogelijk lijkt door een combinatie van floating-car-data en traditionele inwinning. De aanbestedingsjurist reageert hier meteen op: *‘Hoe we de dienstverlening kunnen toetsen op innovatieve aspecten is volgens mij de hamvraag’*. Het projectteam besluit zich te richten op publicatie van de aanbestedingsstukken tegen eind februari.

Legitimiteitsassumptie 8:

Innovatieve technieken zijn wenselijk, omdat verkeersmanagers ook tijdens wegwerkzaamheden voorzien blijven van verkeersgegevens.
(normatieve rechtvaardiging)

3.1.2 Rijkswaterstaat sluit zich aan bij het aanbestedingstraject

Terwijl NDW een start maakt met het aanbestedingstraject zit ‘grootaandeelhouder’ RWS niet stil. Een medewerker van de Dienst Verkeer en Scheepvaart (DVS) binnen Rijkswaterstaat, die betrokken is geweest bij de eerste aanbesteding, benadert de RWS-organisaties in Noord- en Oost-Nederland om vertegenwoordigers te sturen voor de NDW-aanbesteding. Eén van deze regionale vertegenwoordigers vertelt dat hij werd

benaderd met de kreet ‘*Tom Poes, verzin een list!*’. Hij en zijn RWS-collega werden geconfronteerd met het krappe budget voor de aanbesteding van hun regio’s. Voor de eerste aanbesteding was een totaalbudget beschikbaar gesteld, waarbij ‘*de grootste hap uit de ruif is genomen door de percelen Zuid en West*’. De RWS’er geeft aan dat het zodoende niet eens mogelijk is om voor NON vast te houden aan dezelfde aanpak als voor de percelen Zuid en West.

‘Als je NDW over het hele rijkswegennet in Oost- en Noord-Nederland zou uitrollen en je zou dat doen volgens de NDW-standaarden⁶⁵ die we toen hadden, dan hadden we drie keer zoveel geld nodig als nu beschikbaar is. [...] Toen hebben wij als Oost- Nederland en Noord-Nederland gezegd: “We willen niet een stukje van ons netwerk hebben, maar we willen gewoon ons hele netwerk hebben dus moeten we wat anders gaan bedenken.” Toen hebben we een driedeling gemaakt: we hebben rustige wegen, waar we niet zoveel hoeven te weten; we hebben drukke wegen, daar willen we juist veel van weten, want dan kunnen we veel doen met verkeersmanagement; en we hebben hele drukke wegen en daar willen we ook ietsje meer van weten. Op die manier, met die gegevensvraag zijn we NDW ingestapt.’

Legitimiteitsassumptie 9:

Verkeersgegevens zijn nodig voor verkeersmanagement.
(normatieve rechtvaardiging)

Afhankelijk van het type weg zal RWS dus genoeg nemen met verschillende soorten verkeersgegevens. Op sommige wegen zijn alleen intensiteiten nodig en op andere zowel reistijden, intensiteiten, puntsnelheden als voertuigcategorieën. Met de munitie in de hand van een aangepaste gegevensvraag op basis van wegcategorisering, last RWS op 18 december 2009 een overleg in met het projectteam. Voor de projectleden is het van te voren niet duidelijk wat het doel is van de bijeenkomst, zo hoor ik van de aanbestedingsjurist. Ook van een RWS’er hoor ik achteraf dat er verschillende percepties heersen over de rol van RWS in het aanbestedingsproces:

‘Als ik nou zelf kijk naar hoe dit hele proces is gelopen, dan heb ik wel heel erg de indruk gehad dat wij toch wel degelijk als projectgroep bezig waren met deze aanbesteding, ook gezien de rol die wij zelf hadden naar onze regionale partners toe.’

⁶⁵ NDW geeft aan dat deze standaarden door RWS aan NDW zijn opgelegd.

[...] Blijkbaar hebben wij duidelijk verschillende visies gehad op wat onze rol nou was tijdens dit proces. Ik heb ons gezien als projectgroep en zij [de aanbestedingsjurist – CvO] heeft ons gezien als een soort inhoudelijke klankbordgroep.’

Aan RWS is de taak om op papier te zetten welke gegevens over welke (delen van) wegen worden gevraagd en van welke kwaliteit de gegevenslevering dient te zijn. RWS is immers wegbeheerder en verkeersmanager van de rijkswegen in Noord- en Oost-Nederland:

‘We hebben dus heel nadrukkelijk gekeken van kunnen we een paar dingen doen, want we wilden graag een stukje innovatie hebben. Op het moment dat we overal lussen gaan neerleggen dan hebben we heel veel lussen nodig en dan wordt het een hele kostbare zaak. Kunnen we nou niet door alternatieve manieren van meten goedkoper gaan meten met minder trammelant in ons asfalt?’

Voor RWS is het belangrijk om de beschikking te krijgen over zowel historische als actuele verkeersgegevens:

‘Op basis van de historie bepaal je hoe weggebruikers zich gedragen op de weg. Daar zit een bepaald omslagpunt in. Je hebt altijd een moment waarop het heel druk is, maar iedereen nog rijdt en dan hoeft er maar een heel klein beetje te veranderen en pats boem, dan staat alles stil. Wat je probeert, is dat punt waarop het allemaal stilstaat te vangen. Dat analyseer je. Dat punt kan je meestal inschatten door de hoeveelheid verkeer of de snelheid die gereden wordt en dat doe je natuurlijk op historische data. Dat moment probeer je aan te geven en dan ga je op basis van de realtime-gegevens monitoren of we die drempel overgaan, ja of nee. Hee piep, ik ga mijn drempel over, nou moet ik een maatregel in gaan zetten om te voorkomen dat de boel gaat vaststaan. Nou dan

Technologieassumptie 1:

Innovatieve technieken zorgen voor minder wegwerkzaamheden bij de aanleg en het onderhoud van het systeem.

Technologieassumptie 2:

Aan de hand van historische verkeersgegevens kunnen verkeersmanagers een omslagpunt definiëren waarop het verkeer gaat vastlopen.

Technologieassumptie 3:

Op basis van realtime verkeersgegevens kunnen verkeersmanagers een verkeersomslagpunt herkennen in het actuele verkeer.

ga je iets doen, bijvoorbeeld een snelheidsteken aanbrengen of verkeer omleiden, zodat het omslagmoment zo lang mogelijk wordt uitgesteld. Dat doe je op basis van de realtime gegevens.'

Tegelijkertijd is er ook sprake van dat er mogelijk provinciale wegen betrokken gaan worden in de aanbesteding als de provincies Overijssel en Twente zich als nieuwe partners bij NDW gaan aansluiten. Zij willen zich wel aansluiten, maar zich nog niet vooraf vastleggen op mogelijke financiële consequenties, aldus NDW. Dit is een onzekere factor in het aanbestedingstraject, die voor spanningen lijkt te zorgen tussen NDW en RWS. Op een bepaald moment heeft een vertegenwoordiger van RWS het gevoel ingeschakeld te worden als een soort ambassadeur voor NDW. Hij voelt zich echter niet volledig gewaardeerd in die rol:

'In principe is het de taak van NDW om meer regionale overheden te laten aansluiten en warm te maken voor NDW. [...] Men kon echter niet helder maken wat nou de meerwaarde was van NDW en waarom NDW nou zoveel moest kosten en waarom je geld moest betalen voor je eigen informatie. Dat zijn allemaal moeilijke dingen die je in tijden van budgettaire krapte niet verkocht krijgt. [...] Daar was echt zendingswerk te verrichten. Dat begon op een gegeven moment voor mij vrij veel tijd te kosten en toen heb ik tegen NDW gezegd: "ik wil best enthousiasmerend werk voor jullie doen, maar dat moet niet van mij af komen; Daar zijn jullie toch voornamelijk voor."

Begin januari vraag ik aan één van de aanbestedingsjuristen of het projectteam zich blijft baseren op de stukken uit de vorige aanbesteding. Zij zegt dat ze hier nu van gaan afwijken en dat ze dat eigenlijk al eerder had willen doen, omdat de eerste stukken duidelijk voor verbetering vatbaar zijn. In de eerste stuurgroepbijeenkomst die half januari plaatsvindt, *'gaat het erom de uitgangspunten en doelen helder te krijgen, goed te verwoorden en dat de stuurgroep hiermee akkoord gaat'*. De jurist wil voorstellen om de eerder toegepaste bonus-malusregeling niet toe te passen.⁶⁶

Een ander discussiepunt dat ter tafel komt, is het verbod om voor een bepaalde categorie gegevens de traditionele inwinmethode via lusdetectie in het asfalt te gebruiken om zo innovatieve technieken te stimuleren. De achterliggende gedachte is dat de markt wel op zoek moet gaan naar innovatieve inwintechieken als lusingwinning wordt verboden. Het projectteam besluit om innovatie niet expliciet te beoordelen, maar impliciet te stimuleren door gunningscriteria en kwaliteitseisen. De aanbestedingsjurist stelt in een projectvergadering met de heren van RWS:

⁶⁶ Hierbij ontvangt de opdrachtnemer een bonus bij eerder presteren en een boete bij te laat of niet presteren.

‘We gaan innovatie uitlokken door kwaliteitsdifferentiatie plus criteria ten aanzien van hinder en veiligheid. De feitelijke ruimte om innovatieve inwintechniek te krijgen zit hem in de ruimte die de bestekslijst daarvoor biedt’.

Anderhalve maand later spreken het projectteam en RWS af dat RWS de bestekslijsten zo ruim mogelijk gaat opstellen in plaats van per meetpunt te specificeren:

*‘Op die weg willen we dat en dat weten.’
‘Daar wil ik dat hebben op dat kwaliteitsniveau.’*

3.1.3 Tenderboard

Naast een projectgroep en een stuurgroep heeft NDW ten behoeve van de besluitvorming in de aanbesteding een tenderboard opgericht. Deze raad wordt gevormd door een gemêleerd gezelschap qua achtergrond en expertise. De vier heren brengen samen kennis en ervaring op het gebied van inkooptrajecten, innovatie in relatie tot overheidsbeleid en ontwikkelingen in verkeerstechnologie aan tafel. Formeel wordt van hen het volgende verwacht, zo legt de NDW-top uit tijdens de eerste vergadering: *‘Vanuit de eigen expertise meedenken over de aanbesteding en waar nodig verbetervoorstellen doen ten aanzien van de aanbestedingsdocumenten met als doel van de aanbesteding een succes te maken.’* De eerste vergadering van de tenderboard, die op 1 februari 2010 plaatsvindt, wordt als volgt geopend door de NDW-top:

‘Ik ben niet ongelukkig dat er in de vorige aanbesteding maar twee percelen zijn gegund, omdat de technologie zo in ontwikkeling is. Nu kunnen we meer op innovatie sturen. Er zijn twee sessies gehouden waarin we hebben geanalyseerd waarom er geen innovatie uit was gekomen. Risico en kwaliteit waren de twee belangrijkste redenen. Nu is de bedoeling om minimaal datafusie eruit te krijgen.’

Legitimiteitsassumptie 10:

Een innovatieve oplossing mag niet direct worden geëist, maar wel worden gestimuleerd via gunningscriteria. (legaliteit)

Technologieassumptie 4:

Innovatieve technieken stimuleren een gedifferentieerde gegevensbehoefte, zowel qua type als kwaliteit van verkeersgegevens.

Vanuit de projectgroep is er wat scepsis over de waarde van de tenderboard. De één heeft het over ‘*politieke legitimatie die circa anderhalve ton kost*’ en een ander uit twijfels over de mate van bemoeienis van de tenderboard: ‘*de tenderboard is bedoeld om de gang van zaken marginaal te toetsen*’. Ondanks enige weerstand vanuit de projectgroep zorgt de tenderboard al tijdens de eerste vergadering voor een nieuwe draai in het aanbestedingsproces.

Legitimiteitsassumptie 11:

De tenderboard is van belang voor de legitimiteit van de keuze voor een innovatieve oplossing. (maatschappelijke acceptatie)

De tenderboard komt met kritische opmerkingen over het aanbestedingsproces. De suggestie van één van de tenderboardleden dat het wellicht verstandig is om de aanbestedingsprocedure te veranderen van openbaar naar een concurrentiegericht dialoog wordt vervolgens zeer serieus genomen door de NDW-top en geagendeerd voor de stuurgroepvergadering die ruim een week later plaatsvindt.

Kort daarop schrijft de aanbestedingsjurist in een e-mail aan alle tenderboardleden:

‘Tijdens de stuurgroepbijeenkomst van woensdag 10 februari kwam aan de orde dat toch een vorm van marktconsultatie aan de opdracht vooraf zou moeten gaan. Mogelijk wordt daarom bij de aanbesteding gekozen voor een concurrentiegericht dialoog in plaats van een openbare procedure. In verband met deze nieuwe inzichten heb ik de tenderboard bijeenkomst van donderdag 18 februari geannuleerd. Deze week zullen wij op basis van definitieve besluiten over deze koerswijziging een nieuwe planning maken en met alle betrokkenen communiceren.’

Later weet de jurist de NDW-top ervan te overtuigen dat de concurrentiegericht dialoog geen geschikte aanbestedingsvorm is. Aan de dialoog gaat namelijk een selectietraject vooraf. Doordat je dan met enkele potentiële leveranciers verdergaat beperk je de mogelijkheden tot innovatie. In plaats daarvan kan het projectteam wel een marktconsultatie houden en toch vasthouden aan de openbare aanbestedingsprocedure. Op die manier kan toch worden geproefd hoe het voor de markt aantrekkelijk kan worden gemaakt om innovatieve technieken aan te bieden. De marktconsultatie verloopt in twee fasen: afzonderlijke gesprekken tussen het projectteam en zes potentiële aanbieders en een plenaire sessie op de Intertrafficeurs op 24 maart 2010.

3.2 Marktconsultatie

De zes individuele gesprekspartners worden geselecteerd op aanwijzen van het NDW-projectlid. Als reden voor de gemaakte keuze geeft hij aan dat dit de partijen waren die bij de vorige aanbesteding een aanbieding hebben gedaan of anderszins serieuze interesse toonden. De meeste van deze gesprekken vinden plaats op de kantoren van de betreffende bedrijven en vinden plaats met twee à drie vertegenwoordigers. Zelf gaat het projectteam in de hoedanigheid van het NDW-lid en één of twee juristen het gesprek met de marktpartijen aan. In een stuurgroepvergadering op 22 maart 2010 wordt besproken welke inzichten de individuele gesprekken met de markt hebben opgeleverd. Met betrekking tot innovatie maakt de aanbestedingsjurist duidelijk dat kwaliteitsdifferentiatie een geschikt instrument is om innovatie te bevorderen: *‘Marktpartijen zijn van plan om de lagere kwaliteit met innovatieve producten te leveren. Er is dus geen lussenverbod nodig.’*

De plenaire marktconsultatie vindt plaats tijdens de internationale verkeersbeurs Intertraffic. Achter elkaar presenteren de directeur van NDW, de aanbestedingsjurist en de NDW-projectmedewerker. Ze lichten toe hoe NDW na de vorige aanbesteding een aantal innovatiesessies heeft gehouden ter voorbereiding op deze aanbesteding. De jurist geeft aan dat deze bijeenkomst is bedoeld voor het globaal toetsen van de vraag aan het aanbod en niet om in te gaan op specifieke producten. *‘Laten jullie weten waar de schoen wringt en/of waar jullie mogelijkheden zien.’*, zo vraagt ze aan de aanwezige marktpartijen. Hier voegt ze aan toe: *‘Deze bijeenkomst gaat vooraf aan de aanbesteding. Na half april kunnen we niet meer in dit verband bijeenkomen.’* Eén van de marktpartijen stelt al vrij snel een vraag die voor veel geroezemoes in de zaal zorgt: *‘Je hebt het over kwaliteit en wat de eisen zijn van verkeersmanagers, maar hoe zit het met andere afnemers?’*

NDW: *‘Alle gegevens mogen straks worden doorgeleverd.’* Marktpartij: *‘Jullie zeggen min of meer: “het maakt niet uit wat andere afnemers vragen of wensen, we luisteren alleen naar verkeersmanagers, die betalen namelijk.”’* Een andere marktpartij uit eveneens zorgen over dit onderwerp: *‘Ik ben bang dat de eisen teveel vanuit de wegbeheerder worden gesteld, net als bij de vorige aanbesteding.’* NDW geeft aan deze opmerkingen serieus te willen nemen. Marktpartij: *‘Dus de input die wij leveren wordt meegenomen door de wegbeheerder?’* De jurist reageert bevestigend.

Legitimiteitsassumptie 12:

NDW stelt alle verkeersgegevens beschikbaar aan zowel publieke als private afnemers. (legaliteit)

In de planning is voorzien om de resultaten van de marktconsultatie begin april verwerkt te hebben in de aanbestedingsstukken. Deze deadline wordt echter niet gehaald, zo blijkt uit een e-mail van een projectmedewerker op 8 april 2010: *‘We zijn wat vertraagd in de besluitvorming en daardoor is het stuurgroepoverleg op 12 april komen te vervallen’*. De vertraging heeft met name te maken met het nog niet gereed zijn van het RWS bestek.

Op 31 maart 2010 worden tijdens een tenderboardvergadering de concept-aanbestedingsstukken en de resultaten van de marktconsultatie besproken. Een NDW-vertegenwoordiger licht toe:

‘We hebben niet alleen een openbare bijeenkomst gehouden, omdat partijen waarschijnlijk niet het achterste van hun tong zouden laten zien. [...] Over het algemeen kwamen er positieve reacties uit de markt.’

Vervolgens legt de aanbestedingsjurist uit:

‘Nu is het streven dat 80% van de meetlocaties een lage kwaliteit kan hebben. Het uitgangspunt is de informatievraag, niet wat partijen kunnen bieden met hun nieuwste gadgets. [...] In de gesprekken hebben we ook moeten uitleggen dat de partijen een totaal dienstverleningspakket moeten leveren en niet alleen innovatieve techniek moeten hebben. Ze moeten dus ook back-ups maken et cetera.’

Legitimiteitsassumptie 13:

Voor bepaalde wegdelen is het acceptabel dat innovatieve technieken een lagere gegevenskwaliteit opleveren dan traditionele inwintechnieken. (maatschappelijke acceptatie)

Eind april is het eindelijk zover: Onder de titel ‘Inwinnen en verwerken van verkeersgegevens in de Regio’s Noord en Oost Nederland’ wordt de aankondiging gepubliceerd op www.aanbestedingskalender.nl.

3.3 Publicatie, beoordeling en gunning

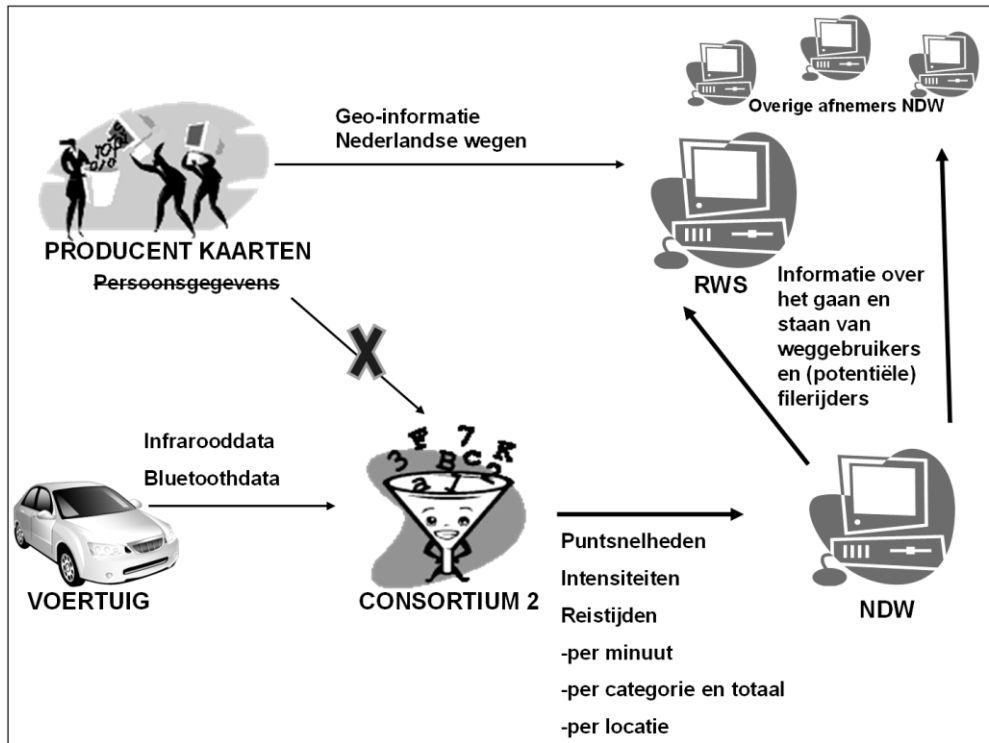
Met de publicatie op de aanbestedingskalender wordt de inschrijving op de opdracht officieel geopend. Vanaf deze website kunnen geïnteresseerde partijen alle aanbestedingsdocumenten downloaden. De Algemene Introductie en Richtlijnen voor de Inschrijving (AIR) is het kerndocument, waaraan onder meer de Statement of Work (SOW) en de bestekslijsten als bijlagen zijn gekoppeld. Geïnteresseerde partijen

hebben vervolgens de gelegenheid om vragen te stellen aan de aanbestedende partij. Van deze gelegenheid wordt gretig gebruik gemaakt. Vervolgens publiceert NDW, eveneens op de aanbestedingskalender, een nota van inlichtingen waarin alle vragen geanonimiseerd worden weergegeven en beantwoord. Naar aanleiding van enkele opmerkingen uit deze nota van inlichtingen wordt op 21 mei 2010 een aangepaste AIR gepubliceerd.

Op 21 juni 2010 ontvangt NDW twee inschrijvingen. Zoals verwacht is er sprake van consortiavorming bij beide aanbiedingen. Consortium 1 wil voor de inwinning van verkeersgegevens gebruik maken van lussen in de weg, GPS en GSM.⁶⁷

Consortium 2 stelt een oplossing voor waarbij gebruik wordt gemaakt van infrarood-technologie en Bluetooth. Op masten van twaalf meter hoog zal, afhankelijk van het aantal te bemeten rijstroken een aantal passieve infrarooddetectoren worden geplaatst om in twee richtingen voertuigpassages te registreren, aan de hand waarvan intensiteiten, voertuigcategorieën en puntsnelheden worden vastgesteld. De masten zijn tevens uitgerust met GPS *‘voor een nauwkeurige tijd en locatie van het systeem’*, zo vermeldt het document met de systeembeschrijving. Om reistijden te verzamelen, scant een Bluetooth-ontvanger Bluetooth-apparaten, zoals carkits en mobiele telefoons. Hierbij worden anonieme, maar unieke MAC-adressen per minuut doorgezonden samen met een tijdsstempel. In de centrale van het consortium wordt steeds een match gezocht in de database, waardoor voor één MAC-adres informatie over start- en eindtijd en start- en eindlocatie beschikbaar komt. De verhouding tussen actoren en gegevensstromen bij het voorstel van consortium 2 is weergegeven in Figuur 6.

⁶⁷ Om redenen van juridische aard worden over de aanbidding van consortium 1 geen verdere technische gegevens vermeld.



Figuur 6: Actoren en gegevensstromen NDW consortium 2

De dag na ontvangst van de twee biedingen komen de drie heren van RWS bijeen op het kantoor van NDW om de biedingen in te zien en hun oordeel af te stemmen. In de formele beoordeling van de inschrijvingen, die enkele dagen later zal plaatsvinden, heeft RWS één van de vier stemmen. Voordat de eerste inzage van start gaat, spreek ik op de gang met de aanbestedingsjurist. Zij geeft aan:

‘Iedereen is opgelucht. Er liggen twee goede aanbiedingen met innovatie erin.’

Tijdens de formele beoordelingssessie die de volgende dag plaatsvindt, moet worden bepaald welke aanbieder het hoogste scoort op de gedefinieerde gunningscriteria. Iedere beoordelaar kent punten toe aan de verschillende gunningscriteria. Het beoordelingscomité bestaat uit drie NDW’ers en één vertegenwoordiger van RWS. Alle vier hebben ze hun waardering voorbereid. De aanbestedingsjurist leidt de beoordelingssessie. Formeel heeft zij geen stem in de beoordeling. Ze geeft aan dat het de bedoeling is om steeds per criterium te bespreken wat eenieder eronder verstaat om vervolgens aan te geven hoeveel punten worden toegekend.

Een lange, spannende en soms verwarrende puntentelling begint. In totaal zijn er maximaal 1000 punten te behalen, verdeeld over drie hoofdcriteria: de mate waarin de aangeboden oplossing hinder veroorzaakt (350 punten), de aannemelijkheid van levering van gegevens (350 punten) en de prijs (300 punten).

‘Tijdens de nota van inlichtingen hebben we criterium 1 nog veranderd. Hinder voor alle locaties laten meetellen, niet alleen op B-locaties.’, geeft de jurist aan. Criterium 1 wordt systematisch doorlopen aan de hand van vooraf gedefinieerde subcriteria, zoals verkeershinder bij aanleg en continuïteit van de gegevensstroom bij wegwerkzaamheden. Soms blijkt de beoordeling lastig te zijn, omdat een aanbieder bepaalde informatie niet expliciet vermeldt. Dit is bijvoorbeeld het geval als het gaat om continuïteit van gegevens bij wegwerkzaamheden.

Technologieassumptie 5:

Innovatieve technieken zorgen voor minder hinder voor wegbeheerder en weggebruiker.

Voorafgaand aan de beoordeling van het criterium ‘aannemelijkheid van de levering van gegevens’ blijkt dat de aanwezigen hiervan verschillende interpretaties hebben. Ter plekke wordt het criterium door de jurist uitgelegd, waarna per subcriterium gezamenlijk punten worden toebedeeld. Steeds vragen de deelnemers zich hardop af: *‘Is het concept overtuigend?’* en *‘Is het waarschijnlijk dat het concept gaat werken?’*. De beoordelaars bespreken per aanbidding een aantal opvallende zaken. De jurist noteert steeds alle argumenten ten behoeve van de formele toe- of afwijzing.

Na de puntentelling komt consortium 1 met slechts tien punten verschil ten opzichte van de concurrentie als winnaar uit de bus (723 tegen 713 punten). Maar dan grijpt de aanbestedingsjurist in. Wanneer de aanbestedingscriteria nogmaals worden doorgenomen blijkt consortium 1 alsnog niet te voldoen aan de aanbestedingseis van het hebben van aantoonbare ervaring als business-to-business dataprovider. De jurist legt uit:

Legitimiteitsassumptie 14:

NDW accepteert een innovatieve oplossing alleen als de leverancier een ervaren business-to-business dataprovider is. (legaliteit)

‘Dit is belangrijk, omdat een ander consortium zal vragen welke drie projecten het gewonnen consortium heeft ingediend als referentie. Dan hebben we een serieus probleem. Dit is het verschil tussen afwijzen en gunnen.’

Het gaat hierbij niet om een gunningscriterium waarop gescoord kan worden, maar om een minimumeis waar een aanbieder aan moet voldoen. In eerste instantie was de aanbidding van consortium 1 door deze eerste keuring heen gekomen. Nu deze aanbidding alsnog wordt afgekeurd, wordt de beoordeling van de gunningscriteria in één klap irrelevant. *By default* wint consortium 2, waar serviceprovider X geen deel van uitmaakt, alsnog. Zodoende bereikt NDW de zo nagestreefde innovatie, maar speelt de politiek gewenste serviceprovider X uiteindelijk geen rol in de realisatie daarvan. Voorts maakt NDW zich enige zorgen over de verantwoording hiervan, zo blijkt uit een uitspraak tijdens de stuurgroepvergadering waarin de beoordeling van de aanbiddingen wordt besproken: *‘Maar de minister is vrienden met serviceprovider X, dus we moeten wel een goed verhaal hebben.’*

In dezelfde vergadering is er kort aandacht voor de verantwoording over een ander onderdeel van de winnende aanbidding: privacyaspecten van de aangeboden technieken.

NDW: *‘Ik zie privacy niet terugkomen in de stukken. Is hier aandacht aan besteed?’*

Jurist: *‘Dat zijn algemene wettelijke randvoorwaarden, net als regels voor werken langs de weg.’*

NDW: *‘Daar komen namelijk wel vragen over in de Tweede Kamer.’*

Deze uiting van zorg over privacyaspecten is opmerkelijk in het licht van een opmerking vanuit NDW tijdens de tenderboardvergadering waarin de concept-aanbestedingsdocumenten werden besproken: *‘De ondernemer moet zelf weten of ze data opslaan of niet. Dat maakt ons niks uit.’*

Eerder laat een beleidsmedewerker van NDW mij al weten:

Legitimiteitsassumptie 15:

NDW moet privacyaspecten van innovatieve technieken kunnen uitleggen aan de Tweede Kamer. (maatschappelijke acceptatie)

Legitimiteitsassumptie 16:

De verantwoordelijkheid voor de privacyaspecten rondom de inwinning en verwerking van verkeersgegevens ligt bij de marktpartij, en niet bij NDW. (legaliteit)

‘Het speelt niet zo bij ons; ik heb de discussie over privacy meer gehoord voor AbvM⁶⁸ en trajectcontroles. We weten door AbvM en trajectcontroles meer wat kan en niet kan. In de zaak Picornie heeft de politie beelden van RWS gebruikt, dat mocht achteraf niet. [...] Het uitgangspunt van NDW is om de burger niet tot last te zijn’.

Uiteindelijk zorgt NDW er evenwel voor dat er een privacyparagraaf wordt opgenomen in de uiteindelijke gunningsovereenkomst. Hierin wijst NDW de opdrachtnemer die de inwinning van verkeersgegevens verzorgt erop dat deze zich moet houden aan de geldende wetten voor de verwerking van persoonsgegevens.

Na consultatie van de tenderboard, die het eens is met de beslissing om te gunnen aan consortium 2, wordt in juli 2010 aan de partijen binnen dit consortium medegedeeld dat zij de opdracht voorlopig gegund krijgen. Op 9 juli 2010 wordt consortium 1 op kantoor bezocht door NDW om het afwijzingsbesluit toe te lichten. De aanbestedingsjurist merkt op dat het afgewezen consortium eventueel bezwaar kan maken tijdens de zogenaamde Alcatel periode. Afhankelijk hiervan gaat het tekenen met consortium 2 de week daarna wel of niet door. Na enkele maanden vertraging vanwege de rechtszaak die consortium 1 inderdaad aanspant en op alle punten verliest, is het dan zover: op 15 oktober 2010 wordt het gunningscontract getekend tijdens een feestelijke ontbijtsessie op het kantoor van NDW. Diezelfde dag vermeldt NDW met trots op haar website: ‘NDW kiest met Data4Traffic⁶⁹ voor innovatieve inwintechnieken’. De zo gewenste innovatie wordt hiermee ingezet.

3.4 Recapitulatie

De Nationale Databank Wegverkeersgegevens streeft innovatie na in de inwinning en verwerking van verkeersgegevens. De innovatiedrang van NDW komt deels voort uit een politieke wens vanuit het toenmalige Ministerie van Verkeer en Waterstaat en deels uit het commentaar van marktpartijen dat NDW de potentie van de markt onvoldoende benut. Van beide zijden wordt het bestaansrecht van de nog jonge uitvoeringsorganisatie NDW uitgedaagd.

Door voor de aanbesteding Noord-Oost-Nederland een kleiner budget beschikbaar te stellen dan voor de eerste aanbesteding stimuleert RWS/NDW de wegbeheerders om creatiever te zijn in hun gegevensbehoefte, hetgeen directe invloed heeft op de

⁶⁸ Anders betalen voor Mobiliteit.

⁶⁹ Het winnende consortium Data4Traffic bestaat uit de bedrijven Van den Berg Infrastructuren B.V., Swarco AG en VerkeersInformatieDienst B.V.

aanbestedingsvraag. Hierdoor wordt innovatie gestimuleerd. Door daarnaast de mate van hinder bij aanleg en gebruik van het aangeboden systeem tot een belangrijk gunningscriterium te maken, demotiveert NDW het gebruik van technieken die in het asfalt worden aangelegd en stimuleert zodoende het gebruik van innovatieve technologie waarbij dit niet het geval is. Gedurende het aanbestedingstraject heeft NDW extra oog voor één bepaalde potentiële aanbieder van innovatieve technologie: serviceprovider X. NDW veronderstelt dat het politiek wenselijk is dat dit bedrijf onderdeel uitmaakt van de winnende aanbidding. Wanneer blijkt dat serviceprovider X geen partij is in het winnende consortium heeft NDW ondanks de euforie over de bereikte innovatie toch het gevoel iets uit te moeten leggen. Hierin wordt de spanning zichtbaar tussen de juridische legitimiteit van de aanbestedingsprocedure en de maatschappelijke legitimiteit van de goedkeuring door de politieke autoriteiten.

Hoe kunnen de bij het innovatiebeleid behorende mobiliteitsgegevens worden gekwalificeerd?

Objectgegevens	
Artefact (Apparaatgegevens)	<ul style="list-style-type: none"> - Aanwezigheid voertuig - Lengtecategorie voertuig - MAC-adres Bluetooth-apparaat
Lichaam (Persoonsgegevens)	<ul style="list-style-type: none"> - Geen
Actie (Situationele identiteit)	<ul style="list-style-type: none"> - Weggebruiker - Potentiële filerijder
Locatiegegevens	
Ruimtelijk (Coördinaten)	<ul style="list-style-type: none"> - GPS-gegevens meetlocatie
Netwerk (Cell-topologie)	<ul style="list-style-type: none"> - Geen
Beschrijvend (Geografische verwijzing)	<ul style="list-style-type: none"> - Wegnummer - Naam knooppunt - Hectometerpaal
Tijdsgegevens	
Heden (Realtime ingewonnen gegevens)	<ul style="list-style-type: none"> - Actuele drukte op de weg t.b.v. verkeersmanagement en verkeersinformatie
Verleden (Opgeslagen gegevens)	<ul style="list-style-type: none"> - Historische wegverkeersgegevens
Toekomst (Gecalculeerde gegevens)	<ul style="list-style-type: none"> - Verwachte filevorming

Tabel 14: Mobiliteitsgegevens bij verkeersinnovatie

Tabel 14 laat zien dat het surveillanceobject als artefact en actie gekwalificeerd wordt. NDW is voornamelijk geïnteresseerd in locatie- en tijdsgegevens over artefacten: (categorieën) voertuigen en Bluetooth-apparatuur. Bij het toepassen van deze gegevens voor verkeersmanagement maakt RWS de vertaling van artefactgegevens naar actiegegevens. RWS wil locatie- en tijdsgegevens hebben over weggebruikers en meer specifiek (potentiële) filerijders. Noch NDW, noch RWS heeft belangstelling voor personen als surveillanceobject. De identiteit, lichaams- of groepskenmerken van een bestuurder zijn niet relevant voor het innovatiebeleid van NDW. Verder is te zien dat de mobiliteitssurveillance gericht is op het heden, het verleden en de toekomst.

4 Analyse: surveillanceperspectieven in het innovatiebeleid van NDW

4.1 Technologie- en legitimiteitsassumpties

Welke beleidsmatige mogelijkheden ziet NDW met betrekking tot innovatieve technologie? Wat innovatie kan betekenen voor de taakuitoefening van NDW, hangt zowel af van de technische mogelijkheden en beperkingen die NDW toedicht aan innovatieve technologie (technologieassumpties) als van haar ideeën over wat een legitieme inzet van de technologie inhoudt (legitimiteitsassumpties). Tot dusver is duidelijk geworden dat NDW in de ontwikkeling van het innovatiebeleid aandacht besteedt aan enkele wetten, regels en procedures, de focus op innovatieve technologie aan de hand van een aantal (morele) waarden rechtvaardigt en de mening van autoriteiten op een aantal punten van belang acht. Tabel 15 geeft een overzicht van de zes technologieassumpties en zestien legitimiteitsassumpties die in de loop van dit hoofdstuk aan het licht zijn gekomen.

De gevonden technologie- en legitimiteitsassumpties vergelijk ik met de technologie- en legitimiteitsassumpties die ik in hoofdstuk 4 per theoretisch surveillanceperspectief heb vastgesteld. Hierdoor wordt inzichtelijk op welke punten de beleidsontwikkeling van NDW kenmerken vertoont van de drie surveillanceperspectieven controle, interactie en voorzorg en welke verwachtingen ten aanzien van de relatie overheid-burger uit het beleid spreken.

Technologieassumpties

1. Innovatieve technieken zorgen voor minder wegwerkzaamheden bij de aanleg en het onderhoud van het systeem.
2. Aan de hand van historische verkeersgegevens kunnen verkeersmanagers een omslagpunt definiëren waarop het verkeer gaat vastlopen.
3. Op basis van realtime verkeersgegevens kunnen verkeersmanagers een verkeersomslagpunt herkennen in het actuele verkeer.
4. Innovatieve technieken stimuleren een gedifferentieerde gegevensbehoefte, zowel qua type als kwaliteit van verkeersgegevens..
5. Innovatieve technieken zorgen voor minder hinder voor wegbeheerder en weggebruiker.

Legitimiteitsassumpties

1. NDW moet innovatieve technologie inzetten, omdat dit politiek-bestuurlijk wordt verwacht. (maatschappelijke acceptatie)
2. Het is wenselijk dat innovatie geleverd wordt door serviceprovider X. (maatschappelijke acceptatie)
3. NDW moet innovatieve technologie inzetten ten behoeve van haar positie op de verkeersmarkt. (maatschappelijke acceptatie)
4. Innovatie is wenselijk voor het voortbestaan van NDW. (maatschappelijke acceptatie)
5. Door de inzet van innovatieve inwintechnieken kan NDW verkeersgegevens goedkoper inwinnen. (normatieve rechtvaardiging)
6. NDW mag innovatieve technologie alleen inzetten indien deze naar voren komt uit een Europese aanbestedingsprocedure. (legaliteit)
7. Innovatieve technieken zijn wenselijk, omdat ze bijdragen aan de veiligheid van weggebruikers. (normatieve rechtvaardiging)
8. Innovatieve technieken zijn wenselijk, omdat verkeersmanagers ook tijdens wegwerkzaamheden voorzien blijven van verkeersgegevens. (normatieve rechtvaardiging)
9. Verkeersgegevens zijn nodig voor verkeersmanagement. (normatieve rechtvaardiging)
10. Een innovatieve oplossing mag niet direct worden geëist, maar wel worden gestimuleerd via gunningscriteria. (legaliteit)
11. De tenderboard is van belang voor de legitimiteit van de keuze voor een innovatieve oplossing. (maatschappelijke acceptatie)
12. NDW stelt alle verkeersgegevens beschikbaar aan zowel publieke als private afnemers. (legaliteit)
13. Voor bepaalde wegdelen is het acceptabel dat innovatieve technieken een lagere gegevenskwaliteit opleveren dan traditionele inwintechnieken (maatschappelijke acceptatie).

Legitimiteitsassumpties

14. NDW accepteert een innovatieve oplossing alleen als de leverancier een ervaren business-to-business dataprovider is. (legaliteit)
15. NDW moet privacyaspecten van innovatieve technieken kunnen uitleggen aan de Tweede Kamer. (maatschappelijke acceptatie)
16. De verantwoordelijkheid voor de privacyaspecten rondom de inwinning en verwerking van verkeersgegevens ligt bij de marktpartij, en niet bij NDW. (legaliteit)

Tabel 15: Technologie- en legitimiteitsassumpties in het innovatiebeleid van NDW

4.2 Koppeling aan surveillanceperspectieven

4.2.1 Kenmerken van het controleperspectief in het innovatiebeleid van NDW

Het controleperspectief is beperkt aanwezig in het innovatiebeleid van NDW. Geen van beide technologieassumpties wordt bevestigd, maar ik vind wel aanwijzingen voor beide aan dit perspectief toebehorende legitimiteitsassumpties. Ik bespreek de bevindingen per assumptie.

Technologieassumptie: wijdverspreide controle van burgers

Het controleperspectief gaat ervan uit dat surveillancetechnologie de overheid de mogelijkheid geeft om burgers wijdverspreid te controleren op afwijkend gedrag door in de rol van kijker zoveel mogelijk gegevens over zo veel mogelijk burgers als bekeken in te winnen en te verwerken. Deze technologieassumptie manifesteert zich uiteindelijk geenszins in het innovatiebeleid van NDW.

Met de zoektocht naar innovatie lijkt NDW juist een stap te maken van wijdverspreide controle van burgers naar meer gerichte controle. Waar NDW voorheen zoveel mogelijk gegevens wilde hebben over zoveel mogelijk wegen, is ze door de beperkte financiële en technische mogelijkheden van innovatie samen met partner RWS gaan nadenken over de werkelijke gegevensbehoefte voor het verkeersmanagement. Aldus versmalt NDW haar blik naar die locaties waarvan ze verwacht dat er mogelijk ingegrepen moet worden: de risicowegen. De zoektocht naar innovatie brengt een overgang teweeg van een controleperspectief op de toepassing van verkeersgegevens naar een voorzorgperspectief.

Daarbij maakt RWS het zich met de NDW-werkwijze voor het verkrijgen en verwerken van gegevens onmogelijk om individuele burgers op afwijkend gedrag te controleren. De Bluetooth-metingen vinden weliswaar op individueel voertuigniveau plaats, maar de bijbehorende unieke MAC-adressen worden vernietigd, nadat de dataprovider de benodigde berekeningen voor het bepalen van reistijden heeft uitgevoerd. NDW ontvangt alleen reistijdinformatie tussen twee locaties en heeft haar eigen systeem niet ingericht op het ontvangen van individuele mobiliteitsgegevens. Voor de infraroodmetingen geldt dat deze slechts de aanwezigheid, lengte en snelheid van een passerend voertuig kunnen vaststellen. Voor deze gegevens geldt eveneens dat deze geaggregeerd per minuut worden doorgeleverd aan NDW. Zodoende ontvangt NDW iedere minuut per meetlocatie en per rijstrook gegevens over het totaal aantal voertuigen, het aantal voertuigen per lengtecategorie, de hoogste, laagste en gemiddelde puntsnelheid.

Technologieassumptie: disciplineren van burgers

Uit het casusmateriaal volgen geen aanwijzingen dat NDW veronderstelt dat een innovatief inwinsysteem de mogelijkheid zou geven om burgers te disciplineren. Burgers zijn zich weliswaar bewust van het feit dat Rijkswaterstaat hun normen kan opleggen, zoals een aangepaste maximumsnelheid of route, als de verkeerssituatie daartoe aanleiding geeft, maar NDW laat hun niet weten dat dit meer en meer gebeurt op basis van innovatief ingewonnen gegevens over hun voertuigbewegingen.

Legitimiteitsassumptie: inzet van surveillance ten aanzien van burgers

De casus laat zien dat NDW in haar beleidsvorming aandacht besteedt aan de juridische, normatieve en maatschappelijke gronden waarop innovatieve inwintechnieken worden ingezet. Deze legitimiteitsassumptie manifesteert zich door de volgende veronderstellingen in het innovatiebeleid van NDW:

Legaliteit

- NDW mag innovatieve technologie alleen inzetten indien deze naar voren komt uit een Europese aanbestedingsprocedure.
- Een innovatieve oplossing mag niet direct worden geëist, maar wel worden gestimuleerd via gunningscriteria.

Normatieve rechtvaardiging

- Door de inzet van innovatieve inwintechneken kan NDW verkeersgegevens goedkoper inwinnen.
- Innovatieve technieken zijn wenselijk, omdat ze bijdragen aan de veiligheid van weggebruikers.
- Verkeersgegevens zijn nodig voor verkeersmanagement.

Maatschappelijke acceptatie

- NDW moet innovatieve technologie inzetten, omdat dit politiek-bestuurlijk wordt verwacht.
- NDW moet innovatieve technologie inzetten ten behoeve van haar positie op de verkeersmarkt.
- Het is wenselijk dat innovatie geleverd wordt door serviceprovider X.
- Innovatie is wenselijk voor het voortbestaan van NDW.
- De tenderboard is van belang voor de legitimiteit van de keuze voor een innovatieve oplossing.

Aan de hand van deze veronderstellingen legitimeert NDW voor zichzelf en naar buiten toe dat ze innovatie in de inwinning van verkeersgegevens nastreeft. Er ontstaat een spanning tussen de legaliteit van de aanbestedingsprocedure en maatschappelijke acceptatie van levering door serviceprovider X wanneer blijkt dat serviceprovider X geen onderdeel uitmaakt van het winnende consortium.

Legitimiteitsassumptie: beschermen van privacy van burgers

De bescherming van de privacy van burgers krijgt enige aandacht in de beleidsvorming, maar niet zeer uitgebreid. De assumptie dat aandacht voor privacy van belang is bij de inzet van surveillance komt als volgt tot uiting:

Legaliteit

- De verantwoordelijkheid voor de privacyaspecten rondom de inwinning en verwerking van verkeersgegevens ligt bij de marktpartij, en niet bij NDW.

Maatschappelijke acceptatie

- NDW moet privacyaspecten van innovatieve technieken kunnen uitleggen aan de Tweede Kamer.

NDW geeft aan dat er geen gevaar is voor privacy bij de verwerking van verkeersgegevens door NDW, omdat NDW deze geanonimiseerd ontvangt. De marktpartijen die de inwinning van verkeersgegevens verzorgen moeten zich toch gewoon aan de geldende wetten voor de verwerking van persoonsgegevens houden. NDW wijst hierop in de gunningsovereenkomst. Enerzijds duidt dit erop dat NDW vertrouwen heeft in de geldende wetgeving op het gebied van privacy en de verwerking van persoonsgegevens, anderzijds is NDW duidelijk van mening dat de verantwoordelijkheid hiervoor niet bij henzelf ligt.

4.2.2 Kenmerken van het interactieperspectief in het innovatiebeleid van NDW

Ook het interactieperspectief is aanwezig in het innovatiebeleid van NDW. Ik vind geringe bevestiging van beide legitimiteitsassumpties en niet van de technologie-assumpties. Ik bespreek de bevindingen per assumptie.

Technologieassumptie: verbinden van overheid en burgers

Dat surveillancetechnologie overheid en burgers met elkaar in verbinding zou kunnen brengen, komt niet terug in het innovatiebeleid van NDW. Voor NDW zijn burgers slechts indirecte afnemers van de gegevensproducten die ze levert aan wegbeheerders en serviceproviders. Ook Rijkswaterstaat, die wel direct te maken heeft met burgers als weggebruikers, ziet innovatieve technologie op dit moment niet als een verbindende schakel. Wel is RWS zich bewust van de voordelen die innovatie met zich meebrengt voor weggebruikers in de zin van minder hinder bij aanleg en onderhoud van het systeem dan bij traditionele inwinsystemen. Ten tijde van het casusonderzoek richt RWS zich niet op het maken van nieuwe verbindingen met burgers door middel van innovatieve technologie, maar is zich wel bewust van ontwikkelingen rondom coöperatieve verkeerssystemen, waarmee wel nieuwe verbindingen kunnen worden gelegd tussen voertuigen onderling en tussen voertuigen en verkeersmanagement-systemen.

Technologieassumptie: gezamenlijke informatiecreatie

Surveillancetechnologie stelt overheid en burgers in staat om informatie over zichzelf en elkaar te creëren, te beoordelen en aan te passen, zo luidt deze assumptie. Deze assumptie komt tot uiting in het innovatiebeleid van NDW in die zin dat NDW ervan uitgaat dat verkeersgegevens tot stand komen door fusie van gegevens die ingewonnen zijn door verschillende technologieën. Zodoende wordt technologie zelf een actor in het proces van gegevenscreatie. Burgers spelen in de ogen van NDW vooralsnog een

passieve rol in dit proces. Ook al ziet NDW in dat de gegevens die over burgers worden verzameld indirect bij hen terugkomen in de vorm van verkeersinformatie, ziet ze burgers niet als prosumers van deze informatie.

Legitimiteitsassumptie: toegang tot surveillance-informatie

Deze legitimiteitsassumptie speelt een rol in het innovatiebeleid, omdat het voor marktpartijen belangrijk is in hoeverre de door hen geleverde verkeersgegevens door NDW beschikbaar worden gesteld aan andere marktpartijen.

Legaliteit

- NDW stelt alle verkeersgegevens beschikbaar aan zowel publieke als private afnemers.

Deze assumptie vloeit voort uit afspraken in het Strategisch Beleid Verkeer en Vervoer (SBVV), waar markt en overheid aan tafel zaten. Deze regel helpt NDW in haar streven naar een centrale positie in de markt voor verkeersgegevens. Enerzijds krijgt de rijksoverheid zodoende meer regie op de tot dusver versnipperde lokale praktijken van wegbeheerders. Anderzijds krijgt ze weer een vinger in de pap in de geprivatiseerde markt voor verkeersinformatie, die enkele jaren eerder juist uit overheidshanden was weggehaald. Voor NDW is de discussie over toegang tot gegevens relevant voor het innovatiebeleid. Bepaalde marktpartijen, waarvan NDW hoopt en verwacht dat ze een innovatieve aanbidding zullen doen, vinden het namelijk problematisch als NDW de door hen ingewonnen gegevens doorverkoopt aan concurrerende marktpartijen.

Legitimiteitsassumptie: relevantie en kwaliteit van surveillance-informatie

De relevantie en kwaliteit van de te leveren gegevens is een centraal onderwerp in het innovatiebeleid. Lange tijd maakt NDW zich zorgen dat innovatieve technieken een te lage gegevenskwaliteit zullen opleveren om van betekenis te kunnen zijn voor het verkeersmanagement door wegbeheerders. Op een later moment in het aanbestedingsproces blijkt deze verwachte eigenschap van innovatieve inwintechieken juist één van de sleutels te zijn om innovatieve biedingen uit te lokken. NDW krijgt steun vanuit de RWS-achterban om kwaliteitsdifferentiatie door te voeren in de gegevensvraag. Op 20% van de aanbestede wegen wordt een hoge gegevenskwaliteit gevraagd (A-kwaliteit) en op 80% een lagere B-kwaliteit, waarbij NDW ervan uitgaat dat

innovatieve technieken alleen de B-kwaliteit kunnen leveren.⁷⁰ Het belang van de relevantie en kwaliteit van verkeersgegevens in het innovatiebeleid van NDW komt in de volgende veronderstellingen tot uiting:

Legaliteit

- NDW accepteert een innovatieve oplossing alleen als de leverancier een ervaren business-to-business dataprovider is.

Normatieve rechtvaardiging

- Innovatieve technieken zijn wenselijk, omdat verkeersmanagers ook tijdens wegwerkzaamheden voorzien blijven van verkeersgegevens.

Maatschappelijke acceptatie

- Voor bepaalde wegdelen is het acceptabel dat innovatieve technieken een lagere gegevenskwaliteit opleveren dan traditionele inwintechieken.

4.2.3 Kenmerken van het voorzorgperspectief in het innovatiebeleid van NDW

Het voorzorgperspectief manifesteert zich op een aantal punten in het innovatiebeleid van NDW. Ik vind bevestiging van alle technologieassumpties, maar niet van de legitimiteitsassumptie. Ik bespreek de bevindingen per assumptie.

Technologieassumptie: identificeren van risico's en risicoburgers

De assumptie dat surveillancetechnologie de mogelijkheid geeft om risico's en risicoburgers te identificeren, komt in twee beleidsveronderstellingen naar voren:

- Innovatieve technieken stimuleren een gedifferentieerde gegevensbehoefte, zowel qua type als kwaliteit van verkeersgegevens.
- Aan de hand van historische verkeersgegevens kunnen verkeersmanagers een omslagpunt definiëren waarop het verkeer gaat vastlopen.

⁷⁰ Overigens blijkt de leverancier uiteindelijk overall de A-kwaliteit te kunnen leveren, zo laat NDW mij eind 2013 weten.

De contouren van het te identificeren risico zijn weliswaar bekend, maar de precieze parameters van het risico worden vastgesteld aan de hand van historische verkeersgegevens over een bepaalde locatie. Er is een punt waarop het verkeer dreigt vast te staan, maar welk punt dit waarschijnlijk is, wordt op deze manier bepaald. Surveillancegegevens helpen zodoende om het risico op filevorming beter in kaart te brengen. Burgers worden risicoburgers op het moment dat hun gedrag zich binnen de risicoparameters betreft puntsnelheden en intensiteiten begeeft (surveillanceobject op actieniveau).

Technologieassumptie: beteugelen van risico's

Ook de tweede technologieassumptie binnen het voorzorgperspectief komt tot uiting in het innovatiebeleid van NDW. In de ogen van NDW geven innovatieve technieken enerzijds de mogelijkheid om het inmiddels bekende risico op filevorming te beteugelen en anderzijds om risico's tegen te gaan die traditionele inwinsystemen wel met zich meebrengen. De volgende beleidsveronderstellingen wijzen hierop:

- Innovatieve technieken zorgen voor minder wegwerkzaamheden bij de aanleg en het onderhoud van het systeem.
- Innovatieve technieken zorgen voor minder hinder voor wegbeheerder en weggebruiker.
- Op basis van realtime verkeersgegevens kunnen verkeersmanagers een verkeersomslagpunt herkennen in het actuele verkeer.

Actuele verkeersgegevens bieden verkeersmanagers de mogelijkheid om acute risico's op filevorming te herkennen en hier vervolgens naar te handelen om te voorkomen dat deze daadwerkelijk optreden. Door middelen als snelheidsbeperkingen en wegomleidingen proberen verkeersmanagers automobilisten met de dubbele status van risicoburger (oorzaak van mogelijke file) en risicolopende burger (lijdend onder mogelijke file) weer risicovrij te maken. Een ander type risico's dat wordt tegengegaan door het type apparatuur van de innovatieve inwinsystemen, en niet zozeer door de gegevens van deze systemen, is het risico op hinder, zoals wegafsluitingen en -werkzaamheden. De achterliggende gedachte is dat innovatieve inwinsystemen doorgaans niet in het asfalt, en ook minder in de buurt van het asfalt geplaatst worden dan traditionele inwinsystemen. Zodoende wordt hiermee het risico op hinder bij aanleg en onderhoud verkleind.

Legitimiteitsassumptie: definiëring van risico's en risicocategorieën burgers

NDW besteedt in de beleidsvorming over innovatie weinig aandacht aan de gronden waarop risico's en risicocategorieën burgers worden gedefinieerd. Het zijn de verkeersmanagers van de partners (waarvan RWS de grootste is) die op basis van hun verkeerskundig inzicht de door NDW ingewonnen gegevens interpreteren om risico's te herkennen.

4.2.4 Overzicht van surveillanceperspectieven in het innovatiebeleid van NDW

Het innovatiebeleid van NDW vertoont kenmerken van het controleperspectief, het interactieperspectief en het voorzorgperspectief. Tabel 16 geeft een overzicht van de analyse van surveillanceperspectieven in het innovatiebeleid van NDW.

Technologie- en legitimiteitsassumpties in theorie	Manifestatie in innovatiebeleid NDW
Controleperspectief	
Wijdverspreide controle van burgers	Niet aanwezig
Disciplineren van burgers	Niet aanwezig
Inzet van surveillance ten aanzien van burgers	<ul style="list-style-type: none"> • NDW mag innovatieve technologie alleen inzetten indien deze naar voren komt uit een Europese aanbestedingsprocedure. (legaliteit) • Een innovatieve oplossing mag niet direct worden geëist, maar wel worden gestimuleerd via gunningscriteria. (legaliteit) • Door de inzet van innovatieve inwintechnieken kan NDW verkeersgegevens goedkoper inwinnen. (normatieve rechtvaardiging) • Innovatieve technieken zijn wenselijk, omdat ze bijdragen aan de veiligheid van weggebruikers. (normatieve rechtvaardiging) • Verkeersgegevens zijn nodig voor verkeersmanagement. (normatieve rechtvaardiging) NDW moet innovatieve technologie inzetten, omdat dit politiek-bestuurlijk wordt verwacht. (maatschappelijke acceptatie) • Het is wenselijk dat innovatie geleverd wordt door serviceprovider X. (maatschappelijke acceptatie)

Technologie- en legitimiteitsassumpties in theorie	Manifestatie in innovatiebeleid NDW
Controleperspectief	
	<ul style="list-style-type: none"> • NDW moet innovatieve technologie inzetten ten behoeve van haar positie op de verkeersmarkt. (maatschappelijke acceptatie) • Innovatie is wenselijk voor het voortbestaan van NDW. (maatschappelijke acceptatie) • De tenderboard is van belang voor de legitimiteit van de keuze voor een innovatieve oplossing. (maatschappelijke acceptatie)
Beschermen van privacy van burgers	<ul style="list-style-type: none"> • NDW moet privacyaspecten van innovatieve technieken kunnen uitleggen aan de Tweede Kamer. (maatschappelijke acceptatie) • De verantwoordelijkheid voor de privacyaspecten rondom de inwinning en verwerking van verkeersgegevens ligt bij de marktpartij, en niet bij NDW. (legaliteit)
Interactieperspectief	
Verbinden van overheid en burgers	Niet aanwezig
Gezamenlijke informatiecreatie	Niet aanwezig
Toegang tot surveillance-informatie	<ul style="list-style-type: none"> • NDW stelt alle verkeersgegevens beschikbaar aan zowel publieke als private afnemers. (legaliteit)
Relevantie en kwaliteit van surveillance-informatie	<ul style="list-style-type: none"> • NDW accepteert een innovatieve oplossing alleen als de leverancier een ervaren business-to-business dataprovider is. (legaliteit) • Innovatieve technieken zijn wenselijk, omdat verkeersmanagers ook tijdens wegwerkzaamheden voorzien blijven van verkeersgegevens. (normatieve rechtvaardiging) • Voor bepaalde wegdelen is het acceptabel dat innovatieve technieken een lagere gegevenskwaliteit opleveren dan traditionele inwintechieken. (maatschappelijke acceptatie)

Voorzorgperspectief	
Identificeren van risico's en risicoburgers	<ul style="list-style-type: none"> • Innovatieve technieken stimuleren een gedifferentieerde gegevensbehoefte, zowel qua type als kwaliteit van verkeersgegevens. • Aan de hand van historische verkeersgegevens kunnen verkeersmanagers een omslagpunt definiëren waarop het verkeer gaat vastlopen.
Betugelen van risico's	<ul style="list-style-type: none"> • Innovatieve technieken zorgen voor minder wegwerkzaamheden bij de aanleg en het onderhoud van het systeem. • Innovatieve technieken zorgen voor minder hinder voor wegbeheerder en weggebruiker. • Op basis van realtime verkeersgegevens kunnen verkeersmanagers een verkeersomslagpunt herkennen in het actuele verkeer.
Definiëring van risico's en risicocategorieën burgers	Niet aanwezig

Tabel 16: Surveillanceperspectieven in het innovatiebeleid van NDW

4.3 Implicaties van het innovatiebeleid van NDW voor de relatie overheid-burger

De analyse laat zien dat het innovatiebeleid van NDW kenmerken vertoont van alle drie de surveillanceperspectieven. Zowel het controleperspectief als het interactie- en voorzorgperspectief helpen om de beleidsontwikkeling over innovatie te begrijpen. Wat betekent een innovatiebeleid dat is vormgegeven vanuit alle drie de perspectieven op surveillance nu voor de relatie tussen NDW en burgers? In hoofdstuk 4 heb ik de theoretische implicaties van de verschillende surveillanceperspectieven voor de relatie overheid-burger uiteengezet. Deze theoretische verwachtingen vertaal ik hier naar de empirie van de casus.

4.3.1 Implicaties van het innovatiebeleid van NDW voor de verhouding machthebber-onderdaan

CONTROLEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Surveillance faciliteert en vervangt overheidshandhaving van regelgeving.	Met het beschikbaar komen van NDW-gegevens over met name de tot dusver onbemeten wegen krijgen verkeersmanagers meer munitie in handen om het weggebruik te sturen. In die zin hebben de surveillancegegevens van NDW zeker een faciliterende functie, maar van vervanging van overheidsregelgeving is (nog) lang geen sprake. Het is nog altijd aan de verkeersmanagers zelf om te bepalen welke gegevenswaarden voor hen van belang zijn en of en hoe zij vervolgens reageren als deze optreden. Vooralsnog wordt de maximumsnelheid niet automatisch aangepast op aanwijzing van het surveillancesysteem.
Panoptische disciplineren zorgt ervoor dat burgers overheidsregels naleven.	Rijkswaterstaat zet niet bewust in op disciplineren van burgers, maar het is denkbaar dat het nieuwe inwinsysteem voor verkeersgegevens wel een disciplinerend effect zal hebben. Langs de rijkswegen in Noord- en Oost-Nederland zullen weggebruikers masten zien verrijzen, die eruit zien als meetapparatuur, waardoor ze vermoeden dat ze in de gaten worden gehouden zonder precies te weten hoe het systeem werkt en waarvoor het wordt gebruikt. De websites van NDW en van de bedrijven in het leveranciersconsortium vermelden weliswaar informatie over het systeem, maar dit zijn geen websites die burgers doorgaans bezoeken. Ook RWS heeft vlak na de gunning nog geen plannen ontwikkeld om burgers hierover te informeren.

INTERACTIEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Overheidsregelgeving en -handhaving worden aangevuld door burgernormen en -handhaving.	Het innovatiebeleid van NDW anticipeert niet op een toenemende invloed van burgers op de normstelling door RWS. Mogelijk dat hier verandering in komt met de opmars van coöperatieve verkeerssystemen.
Overheid en burgers stimuleren medeburgers om mee te werken aan handhaving.	Op basis van het innovatiebeleid van NDW is niet te verwachten dat burgers actief betrokken gaan worden bij de handhaving van verkeersnormen op de Nederlandse wegen.
VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Overheidsregelgeving en -handhaving veranderen snel en richten zich op risicogroepen.	Het innovatiebeleid stimuleert RWS om een onderscheid te maken in drie wegcategorieën, afhankelijk van het risico op drukte, en hier vervolgens verschillende geveenseisen aan te verbinden. Bijgevolg wordt over de burgers die op de wegen met een hoog risico rijden meer gegevens verzameld dan over diegenen die zich in minder risicovol gebied begeven. De verkeersmanagers hebben dan ook meer aandacht voor de groepen burgers op risicowegen en zullen hier ook eerder moeten ingrijpen dan op rustige wegen.
Burgers verkeren in Kafkaëske onzekerheid door beperkte kennis over veranderlijke normen.	Wederom geldt deze implicatie niet op individueel niveau, maar geldt mogelijk wel op groepsniveau. De meeste burgers zijn zich er bewust van dat Rijkswaterstaat bij machte is om normen voor het weggebruik te veranderen. Soms kondigt RWS een tijdelijke normverandering, zoals een omleiding vanwege geplande werkzaamheden ruim van tevoren aan, maar dit is niet altijd mogelijk. Als het gaat om acuut dreigende

	<p>risico's op verkeersopstoppen, kan RWS de weggebruiker verrassen met normveranderingen. De onzekerheid voor de weggebruiker zit hem dan in het moment, de duur en de exacte reden van de normverandering. Het is echter waarschijnlijk dat deze onzekerheid van korte duur zal zijn, omdat een groot aantal leveranciers van verkeersinformatie net als RWS afnemers zijn van NDW-gegevens, waardoor ze de weggebruiker tijdig kunnen informeren over de toestand op de weg.</p>
--	---

Tabel 17: Implicaties van het innovatiebeleid van NDW voor de verhouding machthebber-onderdaan

4.3.2 Implicaties van het innovatiebeleid van NDW voor de verhouding dienstverlener -cliënt

CONTROLEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
De overheid verleent toegang tot en gemak bij publieke dienstverlening op basis van surveillancegegevens over burgers.	De hoofddienst die RWS aanbiedt aan de burger is het bevorderen van de doorstroming op de Nederlandse wegen. Uit het innovatiebeleid van NDW vloeit voort dat haar afnemers, waaronder RWS en lokale verkeersmanagers zich gaan baseren op innovatief ingewonnen mobiliteitsgegevens om hun dienstverlening naar burgers toe vorm te geven. Verkeersmanagers analyseren historische NDW-data om hun korte- en langetermijnbeleid op te baseren en maken gebruik van actuele NDW-data om de automobilist een zo goed mogelijke doorstroming te garanderen.
Alle burgers worden reactieve of passieve cliënten.	Burgers worden reactieve cliënten op het moment dat hun wordt gevraagd hun rijgedrag aan te passen, zodat zij gegeven de omstandigheden op de weg zo snel en veilig mogelijk op de plaats van bestemming kunnen geraken. Burgers kunnen eveneens passieve cliënten worden als gevolg van het innovatiebeleid van NDW

	<p>wanneer zij zonder speciale handelingen van henzelf hun bestemming bereiken dankzij ingrepen van verkeersmanagers elders op de weg.</p>
INTERACTIEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
De overheid wordt een passieve, modererende en reagerende dienstverlener.	Er zijn geen aanwijzingen dat RWS met de komst van het innovatieve inwinsysteem passiever wordt in haar dienstverlening naar burgers toe.
Burgers vervangen door prosumptie van surveillance-informatie voor een groot deel de overheidsdienstverlening.	Met de huidige status van innovatie in het verkeersbeleid is tussenkomst van publieke verkeersmanagers onontbeerlijk voor het garanderen van een goede doorstroming. (Voertuigen van) burgers worden door de overheid nog niet gefaciliteerd om mobiliteitsgegevens van medeweggebruikers te ontvangen en hierop te reageren om zo gezamenlijk een goede doorstroming te organiseren.
VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
De overheid biedt dienstverlening selectief en proactief aan afhankelijk van groepskenmerken.	Met de komst van innovatieve inwintechnieken in Noord- en Oost-Nederland krijgen verkeersmanagers verkeersgegevens tot hun beschikking die ze tot op dat moment voor sommige wegen niet hadden en voor andere wegen beperkter hadden. Ze zijn voornemens om aan de hand van deze gegevens filemomenten zo veel mogelijk te voorkomen door tijdig aan de automobilisten die het op dat moment nodig hebben, sturingsinformatie te verstrekken. Zodoende is er zowel sprake van een proactief element als van een benadering op basis van groepskenmerken.

VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Bepaalde groepen burgers worden reactieve of passieve cliënten.	Welke groep op een bepaald moment de verkeersdienstverlening mag genieten, hangt af van de door verkeersmanagers gedefinieerde criteria, zoals snelheid en intensiteit. Een groep ontstaat, zodra bepaalde waarden worden bereikt en bestaat niet meer als de waarden weer normaal zijn. Een automobilist weet dat hij even bij een dergelijke speciale verkeersgroep hoort op het moment dat hij een aangepaste maximumsnelheid ziet verschijnen op de matrixborden of een DRIP in het oog krijgt met route-informatie.

Tabel 18: Implicaties van het innovatiebeleid van NDW voor de verhouding dienstverlener-cliënt

4.3.3 Implicaties van het innovatiebeleid van NDW voor de verhouding democratisch instituut-citoyen

CONTROLEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Door sousveillance maken burgers overheidssurveillance transparant.	NDW houdt zich maar zeer beperkt bezig met wat burgers weten over haar activiteiten, laat staan of ze deze in de openbaarheid brengen. NDW is veel meer geïnteresseerd in de kennis en attitude die politiek (en daarmee indirect burgers), publieke partners en marktpartijen hebben over haar innovatiepraktijken, omdat deze haar hierop kunnen afrekenen.

Sousveillance zet de overheid aan tot verantwoording over de surveillance van burgers.	De sousveillance door politiek, publieke partners en marktpartijen zorgt ervoor dat NDW sterk geneigd is actief te communiceren over haar innovatieambities en stappen om deze te bereiken.
INTERACTIEPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Surveillance faciliteert zelfsturing en coöperatie met de overheid.	Omdat de surveillancegegevens van NDW ook verwerkt worden door producenten van verkeersinformatie, worden burgers indirect gefaciliteerd in zelfsturing. Op basis van de door hen ontvangen verkeersinformatie kunnen weggebruikers hun gedrag aanpassen, uiteraard binnen de bandbreedte van door de overheid opgelegde normen. Het innovatiebeleid impliceert dat verkeersinformatie vollediger en gedetailleerder wordt met de komst van de nieuwe inwinsystemen. Hierdoor worden burgers meer dan voorheen geholpen bij het maken van keuzes in het verkeer.
Burgers eisen een actieve rol op in de handhaving van medeburgers.	Uit het innovatiebeleid van NDW volgen geen aanwijzingen dat burgers op deze manier invulling gaan geven aan hun citizenrol.
VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Risicoanalyses staan centraal in de verantwoording van beleidskeuzes.	Het is zeer waarschijnlijk dat RWS in de verantwoording van haar beleid meer en meer gaat vertrouwen op NDW-gegevens. Besluiten zoals het afsluiten, verbreden en versmallen van wegen of het aanpassen van maximumsnelheden kunnen gemakkelijker dan voorheen worden beargumenteerd aan de hand van de verkregen surveillancegegevens.

VOORZORGPERSPECTIEF	
<i>Theoretische verwachtingen</i>	<i>Empirische bevindingen</i>
Risico's op de publieke agenda bereiken gemakkelijk de surveillanceagenda van de overheid.	Uit het innovatiebeleid volgen geen aanwijzingen dat het publiek invloed heeft op de selectie van risico's die RWS wil gaan beteugelen met de NDW-gegevens. Deze keuze ligt bij de directie en bij de uitvoering binnen Rijkswaterstaat.

Tabel 19: Implicaties van het innovatiebeleid van NDW voor de verhouding democratisch instituut-citoyen

5 Conclusie

De inwinning en verwerking van verkeersgegevens via innovatieve technieken komt tot stand via een samenspel van publieke en private actoren, maar de overheid in de hoedanigheid van NDW is toch sterk sturend. Het beleid van RWS als voornaamste partner van NDW blijkt van doorslaggevende invloed te zijn op het te vormen innovatiebeleid. Opvallend is dat het belang van innovatieve inwintechieken voor andere overheidspartners van NDW en haar private afnemers (producenten van verkeersinformatie) hierin geen rol van betekenis speelt. Een van de belangrijkste vragen in het aanbestedingstraject is hoe NDW de aanbesteding zo kan sturen dat er innovatie uit komt rollen. Hierbij is sprake van de klassieke tegenstelling tussen overheidssturing en het vrije marktmechanisme. Uit het innovatiebeleid van NDW spreken technologieassumpties van het interactieperspectief en het voorzorgperspectief op surveillance. Ingegeven door de zoektocht naar innovatie bij NDW lijkt RWS een stap te maken van wijdverspreide controle van burgers naar meer gerichte controle. Waar RWS voorheen zoveel mogelijk gegevens wilde hebben over zoveel mogelijk wegen, is ze door de beperkte financiële en technische mogelijkheden van innovatie gaan nadenken over de werkelijke gegevensbehoefte voor het verkeersmanagement. Aldus versmalt RWS haar blik naar die locaties waarvan ze verwacht dat er mogelijk ingegrepen moet worden: de risicowegen. De zoektocht naar innovatie brengt een overgang teweeg van een controleperspectief op de toepassing van verkeersgegevens naar een voorzorgperspectief. De legitimiteitsassumpties in het innovatiebeleid zijn echter gerelateerd aan het controleperspectief en het interactieperspectief. De ideeën die NDW heeft over mogelijke beleidstoepassingen van de innovatieve inwin-

technieken sluiten derhalve niet aan bij de criteria die ze van belang acht bij het beoordelen van de legitimiteit. Voor de verhouding machthebber-onderdaan betekent dit dat NDW-gegevens Rijkswaterstaat faciliteren bij het tijdelijk veranderen van verkeersnormen, waarbij meer dan in het verleden de focus ligt op risicowegen en de bijbehorende groepen weggebruikers. In de benadering van cliënten hanteert RWS meer een voorzorgsperspectief dan een controleperspectief. De dienstverlening wordt bij uitstek gericht op die groepen burgers die zich op risicolocaties begeven, om zo te voorkomen dat zij vast komen te staan in het verkeer. De invulling van de verhouding democratisch instituut-citoyen wordt bepaald door de dreiging van sousveillance door politiek en marktpartijen, waardoor NDW zich vooral naar deze partijen toe wil verantwoorden over het verloop en de uitkomst van het innovatiebeleid. Burgers kunnen hun citoyenrol vormgeven, doordat ze meer dan voorheen in staat worden gesteld geïnformeerde beslissingen te nemen over hun weggedrag.

Epiloog

Na tekenen van het gunningscontract in oktober 2010 moet het meetsysteem van Data4Traffic eerst een zogenaamde typetest doorlopen alvorens geïmplementeerd te kunnen worden in Noord- en Oost-Nederland. Bij deze typetest moet de leverancier aantonen dat de geleverde gegevens aan de kwaliteitseisen van NDW voldoen. Na een succesvolle typetest op drie locaties plaatst Data4Traffic in de zomer van 2011 de eerste 50 masten langs de A15 en A28 om een tweede test te kunnen doorlopen: een ketentest waarin de aansluiting op het NDW-systeem wordt getest. De test verloopt naar tevredenheid van NDW, waarna in het voorjaar van 2012 op alle voorziene locaties in Noord- en Oost-Nederland meetapparatuur wordt geplaatst. Op haar website vermeldt NDW (2012) hierover:

‘Er is voor innovatieve technieken gekozen die de wegbeheerder en weggebruiker weinig hinder geven bij de aanleg en tijdens het onderhoud. Er wordt gewerkt met een systeem met draadloze sensoren (infrarood en Bluetooth-meetsystemen), draadloze communicatie (GPRS) en energievoorziening via zonnepanelen. [...] De komende maanden komen de nieuwe verkeersgegevens geleidelijk in de databank. [...] De meetapparatuur registreert geen kentekens en kan niet ingezet worden voor snelheidscontroles. Het gaat enkel om het volgen van verkeersstromen.’

Het is echter maar zeer de vraag in hoeverre weggebruikers kennis nemen van deze toelichting op het nieuwe inwinsysteem.

Op papier is de reikwijdte van NDW zowel qua inwinning en beheer als levering van verkeersgegevens in een paar jaar tijd aanzienlijk toegenomen, zo blijkt uit de informatie op haar website. Van vijftien overheidspartners halverwege 2009 is ze in

vier jaar tijd uitgegroeid naar twintig partners en nog eens vier provincies die alleen aangesloten zijn betreffende wegwerkzaamheden. Inmiddels heeft NDW een nieuwe aanbesteding voor de inwinning en verwerking van verkeersgegevens gestart, omdat het contract met de huidige leveranciers bijna afloopt. Naast een uitbreiding van het inwingsgebied is het aantal afnemers van NDW-gegevens ook toegenomen. Waar NDW begon met een handvol wegbeheerders die haar gegevens wilde hebben blijken nu ook marktpartijen gebruik te maken van NDW-gegevens. Diverse apps, navigatiesystemen, websites, radio- en televisiezenders maken gebruik van NDW-gegevens om het publiek van verkeersinformatie te voorzien.

HOOFDSTUK 8

CONCLUSIE: HET RISICO VAN DE MOBIELE BURGER

1 Inleiding

Dit onderzoek is gestart met de observatie dat er binnen het openbaar bestuur een groeiende interesse bestaat in mobiliteitsinformatie over burgers. Tevens heb ik vastgesteld dat de vraag ‘Wie is waar op welk moment?’ dankzij technologische ontwikkelingen tegenwoordig gemakkelijker en gedetailleerder te beantwoorden is dan ooit. Voorts heb ik het concept publieke mobiliteitssurveillance geïntroduceerd om de technologie en het beleid die met de vraag naar mobiliteitsinformatie over burgers gemoeid zijn in samenhang te kunnen duiden. Als vertrekpunt voor het onderzoek heb ik voor publieke mobiliteitssurveillance de volgende werkdefinitie opgesteld:

Het op digitale wijze verzamelen en verwerken van mobiliteitsgegevens over al dan niet identificeerbare personen, teneinde personen en populaties voor publieke doeleinden te beïnvloeden of te sturen.

De centrale onderzoeksvraag luidt:

Wat zijn de implicaties van publieke mobiliteitssurveillance voor de manier waarop de overheid haar relatie met de burger vormgeeft?

Deze hoofdvraag heb ik uitgewerkt in vijf deelvragen, die richting hebben gegeven aan de voorgaande hoofdstukken. De informatietechnologische kenmerken (hoofdstuk 2) en de politiek-bestuurlijke achtergrond (hoofdstuk 3) van publieke mobiliteits-surveillance zijn aan bod gekomen. Vervolgens heb ik de relatie overheid-burger theoretisch uitgewerkt en heb ik vanuit drie theoretische perspectieven de implicaties van surveillance voor de manier waarop de overheid deze relatie vormgeeft, beredeneerd (hoofdstuk 4). Aansluitend heb ik de onderzoeksmethoden gespecificeerd waarmee ik de empirie van publieke mobiliteitssurveillance heb bestudeerd (hoofdstuk 5). Het empirische deel van dit onderzoek bestaat uit twee casusonderzoeken. De eerste casus behelst de toepassing van automatische nummerplaatherkenning (ANPR) bij een politiekorps (hoofdstuk 6). Als tweede casus heb ik innovatie in de inwinning en verwerking van verkeersgegevens bij de Nationale Databank Wegverkeersgegevens (NDW) besproken (hoofdstuk 7).

In dit hoofdstuk breng ik de opgedane inzichten samen om de centrale onderzoeksvraag te beantwoorden. Tevens reflecteer ik op de onderhavige studie in het licht van de onderzoeksdoelstelling en de wetenschappelijke en maatschappelijke relevantie. Ten eerste leg ik uit wat publieke mobiliteitssurveillance inhoudt in informatietechnologische zin en vanuit haar politiek-bestuurlijke achtergrond. Hiermee beantwoord ik de eerste twee deelvragen van dit onderzoek:

1. Wat is publieke mobiliteitssurveillance in informatietechnologische zin?
2. Wat is de politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance?

In paragraaf 3 behandel ik de overige drie deelvragen van dit onderzoek:

3. Welke perspectieven op surveillance in de relatie overheid-burger kunnen worden onderscheiden?
4. In hoeverre komen de verschillende surveillanceperspectieven voor in de beleidspraktijk van publieke mobiliteitssurveillance?
5. Welke invulling van de relatie overheid-burger vloeit voort uit de in de beleidspraktijk aangetroffen kenmerken van de surveillanceperspectieven?

Aansluitend ga ik in paragraaf 4 in op het antwoord op de centrale onderzoeksvraag. Tenslotte reflecteer ik in paragraaf 5 op de waarde van de uitkomsten van dit onderzoek.

2 ICT en politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance

2.1 ICT van publieke mobiliteitssurveillance

Deelvraag 1 - Wat is publieke mobiliteitssurveillance in informatietechnologische zin?

Met de beantwoording van deze eerste deelvraag heb ik de informatietechnologische kenmerken van publieke mobiliteitssurveillance in kaart gebracht om enerzijds een theoretische fundering van het concept te realiseren en anderzijds de beschrijving van praktijken van publieke mobiliteitssurveillance te faciliteren. In informatietechnologische zin gaat het bij publieke mobiliteitssurveillance om het inwinnen, koppelen en analyseren van gegevens over mobiliteit. De essentie van mobiliteit is de *mogelijkheid* tot bewegen van een object in de dimensies plaats en tijd. Publieke mobiliteitssurveillance heeft daarom net zo goed betrekking op stilstaande als zich verplaatsende personen. Of mensen zich verplaatsen en zo ja, waar en wanneer ze dit

doen, is typisch informatie die met mobiliteitssurveillance verkregen kan worden. Mobiliteit bestaat uit twee aspecten: het surveillanceobject dat (mogelijk) beweegt en de beweging zelf. Mobiliteitsgegevens zijn dan ook gegevens over het surveillanceobject en gegevens van plaats en tijd.

Het surveillanceobject kan een artefact, lichaam en/of actie zijn. Het surveillanceobject kan op drie niveaus worden beschreven: gegevensinwinning, gegevenskoppeling en gegevensanalyse. Plaatsgegevens zijn onder te verdelen in ruimtelijke, netwerk-, en beschrijvende locaties. Gegevens van tijd kunnen het heden, het verleden of de toekomst beslaan. Tabel 20 geeft weer welke soorten mobiliteitsgegevens voorkomen in de twee empirische casussen.

Het inwinnen van mobiliteitsgegevens kan gebeuren met behulp van een scala aan plaatsbepalingstechnologieën: satellietssystemen, netwerktechnologie, overige draadloze technologieën, sensorsystemen, chipkaartsystemen en hybride technologie. In beide casussen wordt gebruik gemaakt van optische sensors om bewegende burgers te lokaliseren. De Politie Noodaalstad maakt gebruik van ANPR en NDW van infraroodtechnologie aangevuld met Bluetooth. De exacte locatie van deze plaatsbepalingstechnologieën is bekend door een GPS-ontvanger. GIS-technologie dient om locatie-, tijds- en objectgegevens te managen, visualiseren en interpreteren tegen de achtergrond van geo-informatie. Hoofdstuk 2 laat eveneens zien dat verschillende actoren een rol spelen in de gegevensketen van inwinnen, koppelen en analyseren van mobiliteitsgegevens: het surveillanceobject, de contentleverancier, de informatieleverancier en de eindgebruiker. Kijkend naar de rollen die overheid en burgers kunnen vervullen, blijkt dat beiden soms meerdere informatierollen tegelijkertijd kunnen hebben. De twee casussen laten zien dat *de* overheid weliswaar meerdere rollen kan vervullen bij het genereren van mobiliteitsinformatie over burgers, maar dat het hierbij in praktijk gaat om verschillende overheidsorganisaties of -afdelingen.

Uit de in hoofdstuk 2 verrichte literatuurstudie blijkt dat het eerste deel van de werkdefinitie van publieke mobiliteitssurveillance een aanpassing behoeft. De omschrijving *‘het op digitale wijze verzamelen en verwerken van mobiliteitsgegevens over al dan niet identificeerbare personen’* blijkt onnodig uitgebreid te zijn. De toevoeging *‘over al dan niet identificeerbare personen’* kan weggelaten worden, omdat mobiliteitsgegevens immers objectgegevens omvatten, waar gegevens over personen weer onder vallen.

	POLITIE-ANPR	NDW-INNOVATIE VERKEERSGEGEVENS
Objectgegevens		
Artefact (Apparaatgegevens)	<ul style="list-style-type: none"> - Foto kentekenplaat - Alfabetieke data kentekenplaat 	<ul style="list-style-type: none"> - Aanwezigheid voertuig - Lengtecategorie voertuig - MAC-adres Bluetooth-apparaat
Lichaam (Persoonsgegevens)	<ul style="list-style-type: none"> - Persoonsgegevens voertuigeigenaar 	Geen
Actie (Situationele identiteit)	<ul style="list-style-type: none"> - Overtreder - Misdadiger - Betrokkene - Aandachtsvestiging - (soms in combinatie met opvallende locatie- en tijdsgegevens) 	<ul style="list-style-type: none"> - Weggebruiker - Potentiële filerijder
Locatiegegevens		
Ruimtelijk (Coördinaten)	<ul style="list-style-type: none"> - GPS-gegevens cameralocatie 	<ul style="list-style-type: none"> - GPS-gegevens meetlocatie
Netwerk (Cell-topologie)	Geen	Geen
Beschrijvend (Geografische verwijzing)	<ul style="list-style-type: none"> - Naam cameralocatie 	<ul style="list-style-type: none"> - Wegnummer - Naam knooppunt - Hectometerpaal
Tijdsgegevens		
Heden (Realtime ingewonnen gegevens)	<ul style="list-style-type: none"> - Hits t.b.v. geplande ANPR-acties - Hits zware delicten t.b.v. ongeplande directe opvolging 	<ul style="list-style-type: none"> - Actuele drukte op de weg t.b.v. verkeersmanagement en verkeersinformatie
Verleden (Opgeslagen gegevens)	<ul style="list-style-type: none"> - Alle passagegegevens (4 maanden) - Passagegegevens verwerkt in het kader van handhaving rechtsorde (6 maanden) 	<ul style="list-style-type: none"> - Historische wegverkeersgegevens
Toekomst (Gecalculeerde gegevens)	<ul style="list-style-type: none"> - Verwachte passages bekende delinquenten 	<ul style="list-style-type: none"> - Verwachte filevorming

Tabel 20: Mobiliteitsgegevens in twee empirische casussen

2.2 Politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance

Deelvraag 2 - Wat is de politiek-bestuurlijke achtergrond van publieke mobiliteits-surveillance?

Hoofdstuk 3 heeft laten zien dat de hedendaagse publieke mobiliteitssurveillance vanuit politiek-bestuurlijk oogpunt te begrijpen is als een resultante van twee ontwikkelingen. Enerzijds is ze een voortzetting van activiteiten die opkomende Europese natiestaten in de zeventiende en achttiende eeuw ontplooiën om hun territoriale grenzen vast te leggen en te bewaken: staatscartografie en de ontwikkeling van het paspoort. Publieke mobiliteitssurveillance is zo gezien een moderne variant van het paspoort, met meer technologische mogelijkheden en toegepast op meerdere domeinen. Anderzijds is publieke mobiliteitssurveillance meer dan een voortzetting van reeds gebaande paden, ook is ze een acceleratie hiervan die is ingegeven door twintigste-eeuwse bedreigingen van de territoriale basis van de staat: explosief toegenomen mobiliteit en de ICT-revolutie. Paradoxaal genoeg is publieke mobiliteitssurveillance derhalve te beschouwen als een reactie op kenmerken van de ICT-revolutie waar ze tegelijkertijd zelf onderdeel van uitmaakt. Publieke mobiliteitssurveillance in combinatie met de toegenomen mobiliteit en vluchtige communicatie van burgers zorgt voor een paradoxale situatie waarin territorialiteit tegelijkertijd belangrijker en minder belangrijk wordt in de relatie overheid-burger. Bij de overheid lijkt een nieuw plaatsdenken te ontstaan waarin plaats als organiserend principe (bijvoorbeeld de vaste route van woninginbrekers of de plaats waar (mogelijk) een file ontstaat) en eenheid van plaats aan belang winnen. Het traditionele belang van macht over plaats is echter nog steeds daar. Burgers lijken zich wellicht minder aan te trekken van territoriale grenzen binnen en tussen landen, maar de overheid is nog altijd volgens dat principe georganiseerd en gelegitimeerd.

Zowel het bepalen van grenzen als het reguleren van mobiliteit, die beide aan de basis liggen van publieke mobiliteitssurveillance, zijn onlosmakelijk verbonden met het wezen van de staat. Staten oefenen macht uit binnen het door nationale grenzen bepaalde gebied en rechtsstaten zijn hierbij gebonden aan de voor hun eigen territorium geldende wet- en regelgeving en stellen deze op. De analyse van de historische ontwikkeling van de cartografie laat zien dat staten steeds meer belang zijn gaan hechten aan het (juridisch) vastleggen van territoriale grenzen ter legitimatie van hun machtsuitoefening. Staten maken kaarten en kaarten maken staten. Kaarten geven politiek-geografische relaties weer en geven ze vorm. Het vastleggen van grenzen op een kaart is soms meer een creatie van de politieke werkelijkheid dan de weergave ervan. Kaarten zijn in de loop der tijd uitgegroeid tot zeer belangrijke informatiebronnen over de wereld en tegelijkertijd vormen ze een mechanisme om diezelfde wereld te ordenen. Grenzen op de kaart geven aan tot waar de legitieme

macht van een staat reikt en tot waar bepaalde rechten en plichten gelden voor de mensen die het territorium betreden of zich al binnen het territorium bevinden. Absolute heersers in het vroegmoderne Europa krijgen met name uit economische en militaire motieven belangstelling voor de handel en wandel van burgers. Hiermee zegt Torpey (2000) dat staten zich het recht hebben toegeëigend om de mobiliteit van hun eigen burgers en die van andere staten te reguleren. Identificatiedocumenten, met name het paspoort, zijn geïntroduceerd om de mobiliteit van (eigen en vreemde) burgers te meten (wie gaan het territorium in en uit) en te managen (wie mogen het territorium in en uit). De groeiende statelijke regulering van mobiliteit gaat hand in hand met een herdefiniëring van het wezen van de staat. Met het ontstaan van de natiestaat wordt aan de notie van *waar* de staat is een notie toegevoegd van *wie* de staat is. Niet langer wordt de staat zuiver gedefinieerd als territorium, maar ook als nationale gemeenschap. Enerzijds is het paspoort een uiting van burgerschap, anderzijds faciliteert het de opvatting van burgerschap als een status die iemand wel of niet kan hebben. Territorialiteit vormt de kern van de staat.

Macht en controle zijn zodoende centrale begrippen om de opkomst van publieke mobiliteitssurveillance te begrijpen. Hoofdstuk 4 laat zien dat deze begrippen ook dominant aanwezig zijn in de theorievorming over surveillance. Ik stel echter vast dat dit controleperspectief alleen onvoldoende handvatten biedt om de hedendaagse publieke mobiliteitssurveillance te begrijpen. Mobiliteitsinformatie wordt tegenwoordig niet zuiver ingewonnen om mobiliteit te controleren. Het gaat nu niet alleen maar om het beschermen van grenzen, maar ook om het reguleren van mobiliteit binnen het territorium ten behoeve van andere publieke belangen. Het interactieperspectief en het voorzorgperspectief op surveillance onthullen in aanvulling op het controleperspectief andere logica's achter de hedendaagse surveillance-activiteiten van de overheid. Welke dit zijn, wordt duidelijk uit de beantwoording van deelvraag 3.

3 Surveillanceperspectieven in theorie en praktijk

3.1 Surveillanceperspectieven in theorie

Deelvraag 3 - Welke perspectieven op surveillance in de relatie overheid-burger kunnen worden onderscheiden?

In hoofdstuk 4 heb ik drie theoretische perspectieven op surveillance onderscheiden: het controleperspectief, het interactieperspectief en het voorzorgperspectief. Deze drie perspectieven heb ik verbonden aan een typologie van de relatie overheid-burger die

bestaat uit drie hoedanigheden waarin overheid en burger zich tot elkaar verhouden: machthebber-onderdaan, dienstverlener-cliënt en democratisch instituut-citoyen.

De drie surveillanceperspectieven geven verschillende beelden van de aard van de surveillancerelatie tussen overheid en burger. Surveillance heeft vanuit ieder perspectief andere kenmerken en daarmee verschillende implicaties voor de relatie overheid-burger. De perspectieven behelzen zowel assumpties over technologie (beleidsmogelijkheden) als over legitimiteit (beoordelingsmaatstaven in termen van legaliteit, normatieve rechtvaardiging en maatschappelijke acceptatie).

Het controleperspectief

Vanuit het controleperspectief is het de vraag hoe de inzet van panoptische surveillance, die burgers controleert en disciplineert versus de bescherming van privacy gelegitimeerd wordt. De frase 'BIG BROTHER IS WATCHING YOU' (Orwell, 1949: 2) is het adagium geworden van het controleperspectief. In het controleperspectief binnen de surveillance studies wordt Jeremy Bentham's stenen panopticon getransformeerd tot een elektronisch superpanopticon. Ten eerste is er nog altijd een tweedeling tussen degenen die kijken en degenen die bekeken worden. Bij surveillance als controle is het in eerste instantie de overheid die kijkt en de burgers die bekeken worden, en niet andersom. Bovendien weet de overheid ook op welke momenten ze wel en niet kijkt. De burger kan er slechts naar raden wanneer iemand in de virtuele wachttorens aanwezig is. Degenen die onder surveillance staan, conformeren zich aan de opgelegde normen, omdat ze altijd gecontroleerd kunnen worden. Informatie- en communicatietechnologie (ICT) stelt de overheid in staat meer en andere kennis over burgers te genereren dan voorheen. De door de overheid gewenste kennis over burgers, wie op welke manier afwijkt van het normale, kan op meer manieren dan ooit worden verkregen.

Het controleperspectief veronderstelt dat surveillancetechnologie de overheid als kijker de mogelijkheid biedt om de burger als bekekene te controleren op afwijkend gedrag (soevereine macht) en te disciplineren (disciplinerende macht). Een centraal vraagstuk over surveillance vanuit controleperspectief is dan ook hoe de macht van de staat gecontroleerd kan worden. Naast de focus op *checks and balances* ten aanzien van de staatsmacht verbindt veel literatuur deze machtsvraag aan het recht op privacy van burgers. Vanuit het controleperspectief faciliteert en versterkt surveillance door de inherente machtsrelatie tussen kijker en bekekene geruisloos de eenzijdige machtsrelatie tussen overheid en onderdaan. Dit gebeurt op het moment dat de machtspositie van de kijker samenvalt met die van de regelgever en handhaver, en die van de bekekene met die van regelkenner en -nalever. De overheid kan haar regelgeving gemakkelijker en uitgebreider handhaven, omdat surveillancetechnologie

de blik van de handhavende functionarissen groter maakt of zelfs vervangt. Tegelijkertijd zorgt surveillance als controle ervoor dat de overheid in feite minder hoeft te handhaven, omdat burgers overheidsregels beter zullen naleven door internalisering hiervan en door de kennis dat ze hierop steeds gemakkelijker gecontroleerd kunnen worden. Vanuit het controleperspectief is surveillance vooral van betekenis voor het gemakkelijk en toegankelijk maken van diensten, waarbij de overheid voornamelijk aanbodgericht te werk zal gaan. Zowel in het toegang geven tot diensten als in het gemakkelijk maken hiervan zijn de surveillancegegevens over burgers het uitgangspunt. Als cliënten hoeven burgers zelf weinig actie te ondernemen om gebruik te maken van de dienstverlening van de overheid. Deze komt vanzelf wel of niet naar hen toe op basis van de gegevens die de overheid over hen heeft. Zodoende worden ze reactieve of zelfs passieve cliënten. Vanuit het controleperspectief heeft de invulling van de citizenrol betrekking op de vraag in hoeverre en op welke manier burgers zelf surveillance kunnen bedrijven jegens de overheid om daarmee tegenwicht te bieden aan de disciplinerende overheidssurveillance. Deze tegensurveillance wordt ook wel aangeduid als *sousveillance*. Door *sousveillance* kan de citizen de transparantie van de overheid vergroten en deze aanzetten tot verantwoording voor de geobserveerde activiteiten.

Het interactieperspectief

Het interactieperspectief, dat surveillance presenteert als verbinder tussen verschillende actoren in de samenleving, richt zich op de vraag hoe toegang tot surveillance en een bepaalde waarde en kwaliteit van informatie gelegitimeerd kunnen worden. De onderkenning dat er een publieke sfeer bestaat waarin burgers in verbinding staan met elkaar en gezamenlijk interacteren, geeft een fundamenteel ander uitgangspunt voor de bestudering van surveillance dan in het controleperspectief. De manier waarop vanuit het interactieperspectief surveillance-informatie tot stand komt, volgt de logica van social media. Surveillance als interactie betekent dat er niet alleen verbindingen tussen burgers onderling ontstaan, maar ook tussen burger en overheid. Het interactieperspectief benadrukt de democratisering van informatie en van surveillance. Informatie over personen is toegankelijk voor velen, komt tot stand door velen en wordt aangepast en beoordeeld door velen. Surveillance-informatie is wijdverspreid evenals de mogelijkheid om in de rollen van kijker en bekekenen bij te dragen aan surveillance. Iedereen kan kijken (naar informatie over anderen) en bekeken worden (op basis van door zichzelf of anderen gedeelde informatie). Vanuit het interactieperspectief wordt verondersteld dat technologie functioneert als verbinder tussen verschillende actoren in de samenleving. Volgens de logica van social media creëren en beoordelen alle gebruikers informatie over zichzelf en over elkaar. Doordat deze informatie gemakkelijk toegankelijk is voor iedereen, wordt surveillance een aangelegenheid voor iedereen. Surveillancetechnologie stelt zowel overheid als

burgers in staat om de rol van kijker aan te nemen en om wat ze zien kenbaar te maken aan iedereen, inclusief de bekekenen. Hierdoor wordt de bekekenen, samen met andere actoren in de samenleving in staat gesteld de betreffende surveillance-informatie te beoordelen, aan te vullen of te corrigeren. Bij legitimiteit vanuit het interactieperspectief gaat het om twee zaken: toegang tot surveillance en de waarde en kwaliteit van surveillance-informatie.

Surveillance als interactie zorgt ervoor dat de burger betrokken raakt bij het maken en handhaven van regels. Gewenst en ongewenst gedrag kan door de overheid, maar met name door medeburgers via social media zichtbaar worden gemaakt. Dit impliceert dat burgers menen in staat te zijn om elkaars gedrag te beoordelen en de plicht of het recht voelen om dit te doen. In sommige gevallen gebeurt dit aan de hand van maatstaven van de overheid, maar er zijn ook situaties waarin medeburgers zelf bepalen wat wel en niet wordt geaccepteerd en vervolgens gerapporteerd. Vanuit interactieperspectief is het begrijpelijk, gemakkelijk en toegankelijk maken van diensten niet exclusief voorbehouden aan de overheid, omdat zij slechts één van de vele actoren is die dienstverleningsinformatie produceert. De burger heeft een dubbelrol als producent en consument (prosumer) van dienstverleningsinformatie. Als cliënt profiteert hij van surveillance-informatie die door medeburgers is gegenereerd. Burgers zorgen er zelf voor dat de juiste dienstverleningsinformatie tot hen komt. De overheid kan in deze als moderator en/of (anonieme) participant fungeren. De burger kan zich manifesteren als citizen door surveillance ten aanzien van zijn medeburgers te initiëren of daaraan mee te werken. De informatie die hierdoor gegenereerd wordt, stelt burgers in staat om elkaars gedrag te beoordelen en wenselijk gedrag te stimuleren. De overheid kan luisteren naar de burger door hem de ruimte te geven tot zelfregulering. Hiermee geeft zij een passieve invulling aan de rol van democratisch instituut. De overheid kan ook de door burgers geuite normen met hen bespreken en meenemen in de vormgeving van overheidshandhaving. In dat geval handelt de overheid in reactie op de onderlinge surveillance tussen burgers.

Het voorzorgperspectief

‘Voorkomen is beter dan genezen’ is het adagium van het voorzorgperspectief op surveillance. Surveillance is te beschouwen als een facilitator van het voorzorgdenken. Het voorzorgperspectief veronderstelt dat surveillancetechnologie risico’s kan helpen identificeren en beteugelen. Bij legitimiteit in dit perspectief gaat het dan ook om het beoordelen van de gronden waarop risico’s en categorieën van burgers worden gedefinieerd. Vanuit het voorzorgperspectief dient surveillance als basis voor interventies. Gegevens worden verzameld, gecategoriseerd en geanalyseerd om beter vooruit te kunnen kijken. Ongemak en onheil moeten niet alleen voorspeld, maar ook voorkomen worden. Om risico’s voor de samenleving inzichtelijk en beheersbaar te

maken, is het categoriseren van burgers essentieel. Surveillance faciliteert dit proces van ‘social sorting’. Uit voorzorg verdienen dergelijke ‘risicoburgers’ meer surveillanceaandacht dan anderen. Surveillancetechnologie heeft in dit perspectief een dubbele functie: zowel het identificeren als het beteugelen van risico’s. Surveillancetechnologie is zodoende te beschouwen als een actor die invloed heeft op de definiëring van risicogroepen door experts en daarmee de agendering van verdergaande surveillance ten aanzien van de betreffende burgers. Risicoburgers krijgen te maken met de tweede functie van surveillance: het beteugelen van risico’s door bepaalde groepen extra in de gaten te houden. Wat er precies voorkomen moet worden en wie hiertoe surveillanceobject moet worden, zijn belangrijke onderwerpen van discussie als het gaat om de legitimiteit van surveillance.

De overheid wil haar onderdanen responsabiliseren om risico’s voor burgers te beheersen en onheil en ongemak voor hen uit te sluiten. Een focus op risicobeheersing impliceert dat regelgeving en handhaving sterk aan verandering onderhevig zijn en worden toegespitst op bepaalde risicogroepen. De onderdaan komt in een onzekere, haast Kafkaëske positie terecht, omdat de regels waar hij zich aan dient te houden veranderlijk zijn. Kennis van risico’s en risicogroepen in de samenleving zorgt ervoor dat de overheid in haar dienstverlening gericht te werk kan en wil gaan. Bepaalde diensten worden toegankelijk gemaakt voor bepaalde groepen burgers. Afhankelijk van de risicogroep waar de burger toe behoort, ontvangt hij diensten van de overheid. De overheid luistert naar de burger en geeft deze een stem in beleidsontwikkeling op het moment dat hij zich opstelt als medevaststeller van risico’s en risicogroepen. Als citoyen verlangt de burger openlijk dat de overheid uit voorzorg adequate maatregelen treft om de door hem geïdentificeerde risico’s te beteugelen. Bij de verantwoording over het gemaakte beleid kunnen surveillancegegevens een belangrijke rol vervullen. De overheid kan zich beroepen op de uitkomst van risicoanalyses via datamining en profiling als grond voor getroffen maatregelen. Tabel 5 aan het eind van hoofdstuk 4 vat samen welke theoretische verwachtingen voor de relatie overheid-burger voortvloeien uit ieder van de drie surveillanceperspectieven.

3.2 Surveillanceperspectieven in de praktijk van publieke mobiliteitssurveillance

Deelvraag 4 - In hoeverre komen de verschillende surveillanceperspectieven voor in de beleidspraktijk van publieke mobiliteitssurveillance?

Deelvraag 5 - Welke invulling van de relatie overheid-burger vloeit voort uit de in de beleidspraktijk aangetroffen kenmerken van de surveillanceperspectieven?

Voor het beantwoorden van deze twee vragen onderzocht ik twee Nederlandse beleidspraktijken van publieke mobiliteitssurveillance. De eerste casus betreft de toepassing van automatische nummerplaattherkenning (ANPR) bij een politiekorps. De tweede casus gaat over innovatie in de inwinning en verwerking van verkeersgegevens in Noord- en Oost-Nederland door de Nationale Databank Wegverkeersgegevens (NDW). Eerst ga ik in op de manifestatie van de verschillende surveillanceperspectieven in de twee beleidspraktijken. In paragraaf 4 bespreek ik de implicaties voor de vormgeving van de relatie overheid-burger, omdat hiermee meteen een antwoord wordt gegeven op de centrale onderzoeksvraag.

In de hoofdstukken 6 en 7 is duidelijk geworden dat het surveillancebeleid in de twee onderzochte casussen technologie- en legitimiteitsassumpties behelst van alle drie de surveillanceperspectieven. De theoretische assumpties komen echter niet in gelijke mate tot uiting in de onderzochte beleidspraktijken. Sommige assumpties heb ik helemaal niet aangetroffen, andere in zwakke mate en andere zijn sterk aanwezig. Tabel 21 laat zien in hoeverre de twee beleidspraktijken technologie- en legitimiteitsassumpties vertonen van de drie surveillanceperspectieven controle, interactie en voorzorg. Hierdoor wordt inzichtelijk welke aannames en veronderstellingen een rol van betekenis spelen in de beleidsvorming over de toepassing van technologie voor publieke mobiliteitssurveillance.

Controleperspectief

Het controleperspectief op surveillance komt met name tot uiting in de criteria die de politie en NDW van belang achten bij de beoordeling van de legitimiteit van hun praktijk van publieke mobiliteitssurveillance. Vooral het verantwoorden van waarom surveillancetechnologie überhaupt mag en moet worden ingezet krijgt in beide casussen ruimschoots de aandacht. Ook is men zich in beide beleidspraktijken bewust van de juridische en maatschappelijke discussie over privacy. De politie schenkt hier in haar ANPR-beleid echter meer aandacht aan dan NDW in haar innovatiebeleid. Voor NDW is privacy minder belangrijk, omdat ze vindt dat de verantwoordelijkheid hiervoor bij marktpartijen ligt. Van de technologieassumpties van het controleperspectief, die de panopticonvisie op surveillance vertegenwoordigen, komt er maar één sterk terug in één surveillancepraktijk. De politie percipieert ANPR heel sterk als een middel om controle en beheersing te verwerven. NDW beschouwt het innovatieve verkeerssysteem in het geheel niet in die termen. Opvallend is dat noch de politie, noch NDW in het surveillancebeleid zinspeelt op de mogelijke disciplinerende werking van hun systemen.

TECHNOLOGIE- EN LEGITIMITEITSASSUMPTIES	ANPR - POLITIE	INNOVATIE - NDW
Controle		
Wijdverspreide controle van burgers (technologieassumptie)	Sterk	Niet
Disciplineren van burgers (technologieassumptie)	Niet	Niet
Inzet van surveillance ten aanzien van burgers (legitimiteitsassumptie)	Sterk	Sterk
Beschermen van privacy van burgers (legitimiteitsassumptie)	Sterk	Zwak
Interactie		
Verbinden van overheid en burgers (technologieassumptie)	Niet	Niet
Gezamenlijke informatiecreatie (technologieassumptie)	Niet	Niet
Toegang tot surveillance-informatie (legitimiteitsassumptie)	Zwak	Sterk
Relevantie en kwaliteit van surveillance- informatie (legitimiteitsassumptie)	Zwak	Sterk
Voorzorg		
Identificeren van risico's en risicoburgers (technologieassumptie)	Zwak	Zwak
Beteugelen van risico's (technologieassumptie)	Sterk	Sterk
Definiëring van risico's en risicocategorieën burgers (legitimiteitsassumptie)	Zwak	Niet

Tabel 21: Empirische manifestatie van surveillanceperspectieven

Interactieperspectief

In geen van beide surveillancepraktijken richt het beleid zich op het aangaan van nieuwe verbindingen tussen overheid en burger of het gezamenlijk creëren van surveillance-informatie. Kortom, er zijn geen technologieassumpties aangetroffen die duiden op een interactieperspectief op surveillance. Wel blijken zowel de politie als NDW oog te hebben voor legitimiteitscriteria die passen bij het interactieperspectief op surveillance. De aandacht voor het al dan niet verlenen van toegang tot surveillance-informatie en de beoordeling van de relevantie en kwaliteit van surveillance-informatie

is in geen van beide casussen ingegeven vanuit een bezorgdheid over de mogelijke invloed van burgers op het surveillancesysteem, maar over de invloed van andere partijen. Met name in de NDW-casus is duidelijk zichtbaar dat de interactie tussen overheid, marktpartijen en de technologie zelf wordt geproblematiseerd.

Voorzorgperspectief

Uit de interpretatieve beleidsanalyse van publieke mobiliteitssurveillance komt naar voren dat de overheid surveillancetechnologie in grote mate associeert met risico's die worden gevormd door mobiele burgers en in mindere mate met de risico's waar mobiele burgers mogelijk mee worden geconfronteerd. In beide onderzochte beleidspraktijken zet de overheid enkele voorzichtige stappen om door gerichte analyse van mobiliteitsgegevens nog onbekende risico's te identificeren. Van datamining en profiling is vooralsnog geen sprake. De overheid is in sterke mate gericht op het beteugelen van bekende risico's. De Politie Noodstad wil met ANPR het risico op bepaalde overtredingen en misdaden beperken en Rijkswaterstaat is voornemens om met innovatieve verkeerstechnologie grip te krijgen op het risico op verkeersopstoppen. Het voorspellen van de aanwezigheid van bepaalde groepen burgers op bepaalde plaatsen en tijden is hiervoor essentieel. Een verschil tussen de casus ANPR en de casus verkeersinnovatie is de manier waarop mobiele burgers worden gezien in termen van risico's. De politie beziet mobiele burgers zuiver als een potentieel veiligheidsrisico. Het zijn de bekende drugsrunners, woninginbrekers en dronken bestuurders wier bewegingen in kaart moeten worden gebracht, omdat zij een mogelijk gevaar vormen voor de samenleving. Uit het innovatiebeleid van NDW spreekt een meer ambigue perceptie van mobiele burgers. Weggebruikers vormen een potentieel filegevaar en moeten hier tegelijkertijd tegen worden beschermd. In deze surveillancepraktijk komen 'control' en 'care' erg dicht bij elkaar, om in termen van David Lyon te spreken. In de politiecassus is er geen sprake van 'care' ten aanzien van mobiele burgers, wel van 'control'. Opvallend genoeg wordt er geen aandacht besteed aan het legitimeren van de gemaakte beleidskeuzes in termen van risicodefinitie en -selectie. Afwegingen over de juridische, normatieve of maatschappelijke gronden waarop risico's zouden kunnen worden gedefinieerd of afgewezen, zijn blijkbaar niet van belang bij de legitimering van het surveillancebeleid. Risicodefinitie lijkt vooralsnog een politieke of technocratische aangelegenheid te zijn. Zodoende blijft het impliciet op grond waarvan bepaalde groepen burgers mogen of moeten worden gesurveilleerd.

De in de beleidspraktijk aangetroffen assumpties over de technologie en de legitimiteit van publieke mobiliteitssurveillance brengen een aantal implicaties met zich mee voor de manier waarop de overheid invulling geeft aan de relatie overheid-burger. Hiermee kom ik op de beantwoording van de centrale onderzoeksvraag.

4 Implicaties van publieke mobiliteitssurveillance voor de manier waarop de overheid haar relatie met de burger vormgeeft

Op basis van het theoretisch en empirisch onderzoek dat ik heb verricht kom ik tot de conclusie dat de manier waarop publieke mobiliteitssurveillance gestalte krijgt zich kenmerkt door een beperkte aansluiting tussen de aan het beleid onderliggende technologie- en legitimiteitsassumpties, en een tendens van controle naar interactie en voorzorg. Deze twee karakteristieken zijn bepalend voor de manier waarop de overheid haar relatie met burgers vormgeeft. Ik ga allereerst in op deze bepalende karakteristieken en bespreek vervolgens wat deze betekenen voor de invulling van de verhoudingen machthebber-onderdaan, dienstverlener-cliënt en democratisch instituut-citoyen.

Conclusie 1: beperkte aansluiting tussen technologie- en legitimiteitsassumpties

Kijkend naar welke elementen van de drie surveillanceperspectieven naar voren komen in de onderzochte beleidspraktijken, valt op dat de aangetroffen technologieassumpties veelal niet of slechts beperkt aansluiten op de legitimiteitsassumpties. Zo brengt de zoektocht naar innovatie in de NDW-casus een overgang teweeg van een controleperspectief naar een voorzorgperspectief op de toepassing van verkeersgegevens. De legitimiteitsassumpties in het innovatiebeleid zijn echter gerelateerd aan het controleperspectief en het interactieperspectief. Wat betekent deze observatie nu? Dit betekent dat de overheid veronderstelt dat ze met surveillancetechnologie bepaalde beleidstoepassingen kan realiseren, maar tegelijkertijd hanteert ze criteria van een andere orde om deze toepassingen te legitimeren. Ofwel, de overheid focust op legitimiteitsissues die niet of onvoldoende recht doen aan de technologie-toepassingen die ze voor ogen heeft. De aansluiting tussen technologie en legitimiteit loopt op twee manieren mis. De eerste is een gebrek aan bewustzijn en/of aandacht voor de legitimiteitsissues die gepaard gaan met de beoogde en/of gerealiseerde technologie-toepassingen. De tweede is dat er (nog) geen technologie-toepassing is die aansluit bij de legitimiteitsoverwegingen die richting geven aan het surveillancebeleid. Bij beide vormen van incongruentie worden de checks and balances ten aanzien van het handelen van de overheid discutabel en is de legitimiteit van publieke mobiliteitssurveillance in gevaar.

Conclusie 2: voorzorg en interactie in opkomst

Het controleperspectief helpt implicaties van publieke mobiliteitssurveillance bij politie te begrijpen, maar speelt een meer beperkte rol in de verkeerssector. Voorzorg wordt een steeds dominanter perspectief in de vormgeving van publieke

mobilititeitssurveillance. De beoordeling in termen van legitimiteit blijft hierbij wat achter. Burgers worden steeds meer in termen van risico's gezien en bejegend, maar dit wordt niet passend verantwoord. Het interactieperspectief komt vooralsnog beperkt tot uiting in de onderzochte praktijken van publieke mobilititeitssurveillance. Voor zowel het veiligheidsdomein als het verkeersdomein is echter wel te verwachten dat het interactieperspectief zich zal laten gelden bij de vormgeving van publieke mobilititeitssurveillance. In het veiligheidsdomein zijn immers steeds meer praktijken te zien, waarbij de politie burgers betreft bij haar werkzaamheden en deze soms laat overnemen. Zo worden mobiele burgers via Burgernet ingeschakeld om surveillance te verrichten ten aanzien van hulpbehoevende medeburgers zoals vermiste kinderen, of verdachte medeburgers zoals inbrekers (Politie en VNG, 2013). Ook in het verkeersdomein is een ontwikkeling zichtbaar richting meer interactie tussen voertuigen onderling en wegsystemen van verkeersmanagers. Coöperatieve verkeerssystemen zouden hiertoe de sleutel zijn (Wilmink, Immers en Schuurman, 2011).

Conclusie 3: bejegening van de mobiele onderdaan als risico

In de verhouding machthebber-onderdaan wordt de traditionele signaalfunctie van de politie bij de handhaving van regelgeving grotendeels overgenomen door het ANPR-systeem. Daarnaast richt de politie zich in toenemende mate op het tegenhouden van misdrijven en overtredingen door risicogroepen en op risicoroutes. NDW-gegevens faciliteren Rijkswaterstaat bij het tijdelijk veranderen van verkeersnormen, waarbij meer dan ooit de focus ligt op risicowegen en de bijbehorende groepen weggebruikers. In beide beleidspraktijken impliceert publieke mobilititeitssurveillance dat de overheid de mobiele onderdaan als risicoburger benadert. Doordat hij zich op bepaalde momenten op bepaalde plaatsen begeeft, kan een burger worden beschouwd als een risico voor de rest van de samenleving, helemaal als hij ook nog eens over bepaalde objectkenmerken beschikt, zoals een verleden als woninginbreker (politie) of een extra lang voertuig (RWS).

Conclusie 4: streven naar onmerkbare service en bescherming tegen risico's

In de benadering van de mobiele burger als cliënt zijn op hoofdlijnen twee opvattingen waar te nemen. Enerzijds is zowel de politie als RWS van mening dat een groot deel van hun dienstverlening bestaat uit het niet tot last zijn van burgers. In de redenering van de politie is de service aan mobiele burgers dat degenen die niets op hun kerfstok hebben met rust worden gelaten. De burgers die volgens het ANPR-systeem onschuldig zijn, vormen zodoende een groot deel van de clientèle van de politie. Hoe minder deze cliënten persoonlijk te maken krijgen met de politie, hoe groter de service is volgens deze logica. Ook in de NDW-casus is deze opvatting van dienstverlening sterk aanwezig. In het innovatiebeleid wordt er expliciet naar gestreefd dat

weggebruikers zo min mogelijk hinder ervaren van het aan te leggen verkeerssysteem. Daarnaast is het de bedoeling dat de doorstroming op de Nederlandse wegen wordt bevorderd, waardoor weggebruikers zo min mogelijk te maken krijgen met ‘services’ van Rijkswaterstaat, zoals rijstrookafzettingen en aangepaste maximumsnelheden. Naast de onmerkbare service aan mobiele burgers is er een tweede dienstverleningsopvatting waar te nemen in de praktijk van publieke mobiliteitssurveillance. Volgens deze tweede opvatting wordt de mobiele burger als cliënt in bescherming genomen tegen risico’s. Bij de politie is deze opvatting zeer beperkt aanwezig, omdat ze meer een controleperspectief dan een voorzorgperspectief hanteert. Met de inzet van ANPR wil de politie alle burgers in gelijke mate een veilige samenleving garanderen. Op een politieke prominent na wijst ze geen specifieke groepen burgers aan die wellicht bescherming op maat kunnen gebruiken. Dit is anders bij RWS. Deze hanteert meer een voorzorgperspectief dan een controleperspectief in de benadering van cliënten. De dienstverlening wordt bij uitstek gericht op die groepen burgers die zich op risicolocaties begeven, om zo te voorkomen dat zij vast komen te staan in het verkeer (surveillance als ‘care’). In geen van beide casussen kunnen we vervolgens spreken van location-based services van de overheid aan de burger. Waar burgers zich op welke momenten bevinden, is weliswaar informatie die zowel de politie als RWS in toenemende mate voorhanden heeft als gevolg van publieke mobiliteitssurveillance, maar deze wordt vooralsnog beperkt gebruikt om burgers gepersonaliseerd op locatie van dienst te zijn.

Conclusie 5: weinig informatie voor de citizen

Omdat de twee casussen van publieke mobiliteitssurveillance voornamelijk het controleperspectief en het voorzorgperspectief op surveillance laten zien, zal voor menig een de vraag rijzen in hoeverre hier überhaupt sprake is van een verhouding democratisch instituut-citizen. Inderdaad, in geen van beide beleidspraktijken kan de burger stemmen over de inzet van publieke mobiliteitssurveillance of meepraten over de manier waarop de technologie wordt ingezet. Zowel de politie als NDW houdt de burger in deze zin op afstand en lijkt weinig aandacht te besteden aan de burger als citizen. Dit betekent echter niet dat deze overheidsorganisaties helemaal geen invulling geven aan hun rol van democratisch instituut. In het ANPR-beleid van de politie wordt geanticipeerd op de dreiging van sousveillance en bijbehorende mogelijkheid van maatschappelijke en juridische afkeuring van het ANPR-beleid. De politie tast de maatschappelijke acceptatie van met name de proactieve toepassing van ANPR af en wijdt zich aan het opstellen van een juridisch kader. Tegelijkertijd staat de Nederlandse politie klaar om de innovatieve aanpak van bepaalde groepen criminelen wereldkundig te maken. In de NDW-casus wordt de invulling van de verhouding democratisch instituut-citizen bepaald door de dreiging van sousveillance door politiek en marktpartijen, waardoor NDW zich vooral naar deze partijen toe wil verantwoorden

over het verloop en de uitkomst van het innovatiebeleid. In hoeverre burgers op deze manier in staat worden gesteld om invulling te geven aan hun rol als citizen is maar zeer de vraag. Om geïnformeerde beslissingen te nemen over hun weggedrag zijn ze immers afhankelijk van de berichtgeving in de media en van de overheid zelf, die vooralsnog spaarzaam is met informatie over de toepassing van publieke mobiliteits-surveillance.

Overkoepelende conclusie: de mobiele burger als risico

In alle drie de verhoudingen tussen overheid en burger beschouwt de overheid mobiele burgers voornamelijk als potentiële oorzaken van onheil en ongemak. Publieke mobiliteitssurveillance is gericht op de beoordeling van de mobiele burger in termen van een risico voor de samenleving. Zij faciliteert de overheid in het beoordelen van welke mobiele onderdanen mogelijk normen en regels overtreden en zodoende een potentieel gevaar vormen voor de samenleving. Surveillancegegevens helpen de overheid om de risico's die mobiele burgers vormen in kaart te brengen en te beheersen. Ook de mobiele cliënt wordt beoordeeld in termen van risico's en profiteert van onmerkbare dienstverlening als het surveillancesysteem hem niet als risicoburger aanmerkt. Bij de bejegening van de mobiele citizen overheerst eveneens een risicoperceptie. Mobiele burgers worden beperkt geïnformeerd over de overheids-activiteiten in het kader van publieke mobiliteitssurveillance, omdat zij via sousveillance een risico vormen voor de continuering van die activiteiten.

De overheid definieert risico's niet alleen op basis van objectkenmerken van burgers, zoals een verleden als voetbalhooligan of de lengte van het voertuig waar hij in rijdt, maar ook steeds meer op basis van gegevens over de bewegingen van burgers in het verleden en heden. De analyse van kenmerken van bewegingen van (groepen) burgers kan ervoor zorgen dat bepaalde plaatsen (tijdelijk) als risicoplacaten worden aangemerkt, zoals de locatie van een dreigende verkeersopstopping of een populaire route voor bekende drugsrunners.

De conceptualisering van beweging als risico suggereert dat er sprake is van reterritorialisering in termen van een toenemende focus op plaats als organiserend principe: een plaats wordt tijdelijk relevant voor de overheid op het moment dat deze als risicovol wordt bestempeld. Voor de burger betekent deze reterritorialisering dat de overheid hem in toenemende mate als onderdaan aanspreekt op basis van de plaats waar hij zich bevindt, bevond of waarschijnlijk zal bevinden. Daarnaast lijkt er sprake te zijn van reterritorialisering in de zin van een groeiende aandacht voor combinaties van persoons-, locatie- en tijdsgegevens als zijnde risicovol.

In de benadering van burgers en bewegingen als risico's voor de samenleving ontvouwt zich een specifieke interpretatie van het voorzorgperspectief. De voorzorg richt zich voornamelijk op mobiele burgers als risicovormers en in mindere mate als risicolopers. Het beschermen van mobiele burgers tegen de risico's die zij onderweg kunnen lopen, staat niet voorop bij publieke mobiliteitssurveillance. Publieke mobiliteitssurveillance is niet gericht op het uitoefenen van overheidsmacht, het bieden van dienstverlening en verantwoording aan degenen die risico lopen. Kijkend naar de politiek-bestuurlijke achtergrond van publieke mobiliteitssurveillance is de benadering van burgers en bewegingen als risico's frappant te noemen. In de begindagen van het paspoort waren staten gemotiveerd om mobiliteit te reguleren vanwege de mogelijke waarde van burgers voor staat en samenleving. De hedendaagse publieke mobiliteitssurveillance laat eerder een focus zien op de mogelijke schade van de burger voor staat en samenleving.

5 Discussie en reflectie

Welke inzichten heeft dit onderzoek opgeleverd en welke nieuwe vragen roept het op? Ik ga achtereenvolgens in op de waarde van het concept publieke mobiliteits-surveillance en de methodologische benadering hiervan, de surveillanceperspectieven en territorialiteit.

5.1 Het concept publieke mobiliteitssurveillance en de methodologische benadering hiervan

Publieke mobiliteitssurveillance is geen nieuw fenomeen in de praktijk van het openbaar bestuur, maar wel een nieuw concept in de studie van het openbaar bestuur. Wat ik in dit proefschrift aanduid als publieke mobiliteitssurveillance staat derhalve noch binnen het openbaar bestuur zelf, noch in de bestuurskunde als zodanig bekend. Dit onderzoek heeft kennis gegenereerd over het fenomeen publieke mobiliteits-surveillance en tegelijkertijd roept het des te meer vragen op. Wat heeft het gebruik van het concept opgeleverd? Het concept publieke mobiliteitssurveillance heeft het mogelijk gemaakt om de twee uiteenlopende beleidspraktijken van ANPR in het veiligheidsdomein en innovatieve inwintechologie in het verkeersdomein in samenhang te bespreken. In dit onderzoek heb ik eerst laten zien dat deze samenhang vanuit zowel informatietechnologisch als politiek-bestuurlijk oogpunt te motiveren is. Vervolgens heb ik duidelijk gemaakt dat de twee surveillancepraktijken verschillende, maar zeker ook overeenkomstige kenmerken hebben als het gaat om percepties van de

beleidsmogelijkheden van de mobiliteitstechnologie, de beoordeling van legitimiteit en de verhouding tussen beide.

De resultaten van dit onderzoek komen voort uit een interpretatieve beleidsanalyse en dienen ook als zodanig te worden gewaardeerd. De gebruikte methodologie is gericht op begrijpen in plaats van verklaren en op specificeren in plaats van generaliseren. Ik beweer dan ook niet dat er op basis van dit onderzoek universeel geldende uitspraken kunnen worden gedaan over het fenomeen publieke mobiliteitssurveillance. Ik heb me niet gericht op het ontdekken van bepaalde wetmatigheden. Wel is het mijn doel geweest om te komen tot een diepgaand inzicht in enkele praktijken van publieke mobiliteitssurveillance en de beleidsvorming die hiervan onderdeel uitmaakt.

Ik heb de keuze gemaakt om publieke mobiliteitssurveillance in de diepte te onderzoeken en niet in de breedte. Gaandeweg het proefschrift heb ik een aantal verschijningsvormen van publieke mobiliteitssurveillance genoemd, maar ik heb geen systematische studie verricht naar de omvang en de diversiteit van publieke mobiliteitssurveillance in Nederland of in internationaal verband. Met een dergelijke studie had ik weliswaar een *overzicht* verkregen van de hoedanigheden van publieke mobiliteitssurveillance, maar het had geen *inzicht* opgeleverd in de aard van publieke mobiliteitssurveillance en haar betekenis voor de vormgeving van de relatie overheid-burger. De verrichte verkenning van het concept publieke mobiliteitssurveillance biedt theoretische en operationele handvatten om bestaande praktijken te herkennen en deze systematisch in kaart te brengen. De informatietechnologische conceptualisering kan worden gebruikt om de inwinning en verwerking van mobiliteitsgegevens door publieke organisaties te beschrijven om daarmee een overzicht te krijgen van de typen praktijken die er zijn.

Verder biedt het concept publieke mobiliteitssurveillance een gedeeld frame aan beleidsmakers die vanuit hun eigen beleidsterrein naar technologische ontwikkelingen kijken. Overkoepelende problemen op het gebied van legitimiteit, zoals het ontwikkelen van nieuwe wetgeving en het maatschappelijk verantwoorden van bepaalde beleidskeuzes kunnen gemakkelijker samen worden aangepakt.

5.2 Waarde van surveillanceperspectieven: descriptie en duiding

De empirische casussen laten zien dat de drie theoretische surveillanceperspectieven bruikbare handvatten bieden om beleidspraktijken rondom surveillance te duiden en dat het mogelijk is surveillance op een beschrijvende manier te benaderen zonder een bij voorbaat vastgesteld normatief uitgangspunt. Je kan niet zonder meer zeggen: die en

die mobiliteitstechnologie heeft die en die gevolgen voor burgers. Wat de implicaties zijn voor de relatie overheid-burger hangt ten eerste af van de veronderstellingen die beleidsmakers erop na houden betreffende de technologische mogelijkheden en betekenis voor beleid en hun ideeën over wat kan, mag en moet met de technologie. De surveillanceperspectieven helpen om de beeldvorming in de casussen te begrijpen. Het controle-, interactie- en voorzorgperspectief laten verschillende logica's zien waarmee beleidsmakers surveillancetechnologieën benaderen. Afhankelijk van met welke bril een publieke functionaris surveillance beziet (controle-interactie-voorzorg), lijkt hij/zij andere argumenten te hanteren om de inzet van surveillancetechnologie te legitimeren of delegitimeren. De empirie laat zien dat er verschillende logica's tegelijkertijd aan het werk kunnen zijn, waardoor surveillance soms een enigszins schizofreen karakter kan krijgen met ambigue gevolgen voor burgers. Door surveillancebeleid aan de hand van de onderscheiden perspectieven met bijbehorende technologie- en legitimiteitsassumpties te analyseren kunnen tegenstrijdigheden en inconsistenties in het beleid worden blootgelegd. Zodoende biedt dit proefschrift een bestuurskundige aanvulling op technisch, juridisch en ethisch onderzoek.

Het wetenschappelijk debat over surveillance is vaak zeer normatief. Veelal krijgt surveillance bij voorbaat een negatieve kwalificatie. Met dit onderzoek heb ik laten zien dat surveillance prima kan dienen als conceptueel startpunt om overheidsactiviteiten te beschrijven en te begrijpen. In mijn optiek is de gevoerde maatschappelijke en wetenschappelijke discussie vaak te zeer geënt op de technologische, juridische en ethische mogelijkheden en bezwaren en is deze te weinig empirisch gefundeerd. Zodoende krijgt de discussie al snel een normatief karakter, waarbij surveillance bijvoorbeeld slecht zou zijn, omdat de privacy van burgers mogelijk wordt geschaad of juist goed omdat burgers hierdoor zouden kunnen genieten van gepersonaliseerde services. In het denken over de invloed van ICT op de relatie overheid-burger is een polarisering in het debat waar te nemen. Hierbij zijn drie polen te onderscheiden: Orwell, Athene en Soft Sister. Een beperking van de beschreven e-governmentsscenario's is dat ze ieder eenzijdig gefocust zijn op een bepaalde burgerrol. Overheid en burger zijn nader tot elkaar gebracht doordat ik de drie dimensies onderscheid en deze invul in plaats van te zeggen: surveillance zorgt ervoor dat de burger meer of minder onderdaan, cliënt of citizen wordt. Daarnaast worden overheid en burgers meer verbonden in dit thema doordat duidelijk is geworden dat de overheid niet zuiver vanuit het controleperspectief haar surveillancebeleid vormgeeft, maar ook redeneert vanuit andere logica's.

De empirische resultaten maken ook duidelijk dat de surveillanceperspectieven op een aantal punten kunnen worden aangevuld.

- Verbreding begrip interactie: multi-actorbenadering

De praktijken van publieke mobiliteitssurveillance laten zien dat de inzet van surveillancetechnologie in de ogen van publieke organisaties mogelijkheden biedt tot samenwerking met publieke en private organisaties door surveillancedata aan te vullen, te delen en verder te verwerken (technologieassumptie). Daarnaast betekent de samenwerking met andere organisaties een legitimatie voor de inzet van de surveillancetechnologie (legitimiteitsassumptie). Het is goed dat overheidsorganisaties onderling (politie en belastingdienst) en overheid en marktpartijen samenwerken (NDW en dataproviders), zo luidt dan de redenering. Voor het interactieperspectief betekenen deze observaties dat interactie niet alleen begrepen kan worden in termen van interactie tussen overheid en burgers. Interactie gaat ook over verbindingen tussen overheidsinstanties onderling, tussen overheid en marktpartijen en tussen overheid en de technologie zelf. Het controleperspectief en het voorzorgperspectief bezien *de* overheid als een homogene actor. Vanuit het interactieperspectief is het logischer om uit te gaan van verschillende actoren binnen het publieke domein en de nadruk te leggen op de onderlinge interacties om surveillancepraktijken te kunnen begrijpen.

- Uitbreiding surveillanceperspectieven: oogpunt van de burger

In dit onderzoek heb ik publieke mobiliteitssurveillance gezien vanuit het perspectief van de overheid. Vanuit een analyse van hoe de overheid praktijken van publieke mobiliteitssurveillance vormgeeft heb ik implicaties voor de relatie overheid-burger geïdentificeerd. De burger zelf is in dit onderzoek niet aan het woord geweest. In hoeverre burgers als surveillanceobjecten controle, interactie en voorzorg ervaren, en wat deze ervaring betekent voor de manier waarop burgers hun relatie met de overheid vormgeven is uit dit onderzoek niet duidelijk geworden. De toevoeging van het burgerperspectief aan de surveillanceperspectieven zou een waardevolle toevoeging betekenen voor de studie van en het debat over surveillance.

5.3 Publieke mobiliteitssurveillance en de territorialiteit van de overheid

Het valt buiten de reikwijdte van dit proefschrift om in te gaan op de empirische consequenties van publieke mobiliteitssurveillance in termen van territorialiteit. De conclusie maakt duidelijk dat met name het voorzorgperspectief op surveillance aanleiding geeft tot verder onderzoek naar de notie van territorialiteit. Zo constateert Frissen (2013) dat de onvoorspelbare aard van rampen en risico's botst met het maakbaarheidsgeloof van de overheid, waarbij deze alles in het werk stelt om grip te krijgen op het dreigende onheil door tijdig te interveniëren. De organisatie van deze

interventies is doorgaans territoriaal georiënteerd, zoals de 25 veiligheidsregio's die Nederland rijk is. Rampen en risico's houden zich doorgaans echter niet netjes aan de territoriale indeling van de overheid, zeker niet als het mobiele burgers zijn die een risico vormen in de ogen van de staat. Vanuit het voorzorgperspectief op surveillance kan publieke mobiliteitssurveillance de overheid faciliteren in het identificeren en beteugelen van de risico's die worden gevormd door mobiele burgers. Voorts is de vraag hoe het denken in termen van fluïde territorialiteit die deze vorm van surveillance met zich meebrengt, zich verhoudt tot de traditioneel starre notie van territorialiteit die kenmerkend is voor de organisatie van de overheid.

Surveillancesystemen zijn erop gericht om mensen en de problemen die mensen veroorzaken zichtbaar te maken. Om adequaat te kunnen anticiperen en reageren op de zichtbaar wordende mobiele risicoburgers zullen overheidsorganisaties over gemeentelijke, regionale en landelijke grenzen heen moeten samenwerken, maar onder wiens territoriaal gedefinieerde jurisdictie? Wie kan of kunnen legitiem handelen ten aanzien van mobiele risicoburgers en wat gebeurt er als er sprake is van tegenstrijdige legitimiteitspercepties van de betrokken actoren? De spanning tussen fluïde territorialiteit, die ik eerder in dit proefschrift heb besproken aan de hand van plaats als organiserend principe en eenheid van plaats, en vaste territorialiteit verdient het om vanuit organisatorisch en juridisch perspectief te worden geanalyseerd. Als de notie van territorialiteit en die van gemeenschap op losse schroeven staan, wat blijft er dan over van de staat?

LITERATUUR

Aber, J.S. (2004). *History of maps and cartography*. http://academic.emporia.edu/aberjame/map/h_map/h_map.htm (27 juni 2007).

Abma, T.A. en R.J. in 't Veld (red.) (2001). *Handboek beleidswetenschap: perspectieven, thema's en praktijkvoorbeelden*. Amsterdam: Boom.

Ahas, R. en U. Mark (2005). Location based services-new challenges for planning and public administration? *Futures*. 37 (6): 547-561.

Ball, K., E. Daniel, S. Dibb en M. Meadows (2010). Democracy, surveillance and "knowing what's good for you". The private sector origins of profiling and the birth of "Citizen Relationship Management". In: Haggerty, K.D. en M. Samatas (red.) *Surveillance and democracy*. Abingdon: Routledge.

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity*. 10 (1-2): 65-80.

Beetham, D. (1991). *The legitimation of power*. Basingstoke [etc.]: Macmillan.

Bekkers, V., M. Lips en A. Zuurmond (2005a). De januskop van ICT in het publieke domein. In: Lips, M., V. Bekkers en A. Zuurmond (red.) *ICT en openbaar bestuur*. Utrecht: Lemma, 733-751.

Bekkers, V., M. Lips en A. Zuurmond (2005b). De maatschappelijke en politiek-bestuurlijke positionering van ICT in het openbaar bestuur. In: Lips, M., V. Bekkers en A. Zuurmond (red.) *ICT en openbaar bestuur*. Utrecht: Lemma, 17-46.

Bekkers, V. en A. Zuurmond (2005). Achtergronden en eigenschappen van ICT. In: Lips, M., V. Bekkers en A. Zuurmond (red.) *ICT en openbaar bestuur*. Utrecht: Lemma, 49-72.

Bekkers, V. en A. Meijer (2010). *Cocreatie in de publieke sector: een verkennend onderzoek naar nieuwe, digitale verbindingen tussen overheid en burger*. Den Haag: Boom Juridische uitgevers.

Belastingdienst (2012). *Vooraf ingevulde aangifte*. http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/prive/aangifte_doen_belasting_betalen_of_terugvragen/aangifte_inkomstenbelasting_2011/aangifte_doen_over_2011/vooraf_ingevulde_aangifte/ (11 april 2012).

- Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven [Conn.]: Yale University Press.
- Bennett, C.J. en P.M. Regan (2004). Editorial: Surveillance and Mobilities. *Surveillance & Society*. 1 (4): 449-455.
- Black, J. (1997). *Maps and history. Constructing images of the past*. New Haven [etc.]: Yale University Press.
- Black, J. (2004). *Cartografie: de verbeelding van de wereldgeschiedenis*. Warnsveld: Terra.
- Bokhorst, A.M. (2014). *Bronnen van legitimiteit. Over de zoektocht van de wetgever naar zeggenschap en gezag*. Den Haag: Boom Juridische uitgevers.
- Boogers, M. en M. Thaens (2004). *Handvest Digitale contacten tussen burger en overheid*. Universiteit van Tilburg.
- Boomen, M. van den (2007). Van gemeenschap via webnetwerk naar datawolk. In: Steyaert, J. en J. De Haan (red.) *Jaarboek ICT en samenleving*. Amsterdam: Uitgeverij Boom.
- Borgers, M.J. (2007). *De vlucht naar voren*. Den Haag: Boom Juridische uitgevers.
- Bovens, M.A.P. en S. Zouridis (2002). Van street-level bureaucratie naar systeem-level bureaucratie. Over ICT, ambtelijke discretie en de democratische rechtsstaat. *Nederlandsch Juristenblad: weekblad behorende bij de Nederlandsche jurisprudentie*. 77 (2): 65-74.
- Brakel, R. van en P. De Hert (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Journal of Police Studies*. 20 (3): 163-192.
- Bregt, A.K. (2006). Geo-informatie - De emancipatie van locatie. *Geografie: vaktijdschrift voor geografen*. 15 (8): 6-7.
- Brimicombe, A. en C. Li (2009). *Location-based services and geo-information engineering*. Oxford: Wiley-Blackwell.
- Brouwer, E., P. Catz en E. Guild (red.) (2003). *Immigration, Asylum and Terrorism. A Changing Dynamic in European Law*. Nijmegen: Instituut voor Rechtssociologie/Centrum voor Migratierecht KU Nijmegen.

- Brouwer, H.N. (2005). Radio-frequentie identificatie (RFID) en de opsporing: Speech eNederland Conference. *Databodies-l mailinglist*. http://listcultures.org/pipermail/databodies-l_listcultures.org/2006-January/000051.html (6 februari 2008).
- Calabrese, F. en C. Ratti (2006). Real Time Rome. *Networks and Communication Studies. Official Journal of the IGU's Geography of Information Society Commission*. 20 (3&4): 247-258.
- Capling, A. en K.R. Nossal (2001). Death of distance or tyranny of distance? The Internet, deterritorialization, and the anti-globalization movement in Australia. *The Pacific review*. 14 (3): 443-466.
- Castells, M. (2000). *The rise of the network society*. Oxford: Blackwell.
- Clark, S. (1995). *State and status. The rise of the state and aristocratic power in Western Europe*. Cardiff: University of Wales Press.
- Clarke, R. (2003). *Wireless Transmission and Mobile Technologies*. <http://www.rogerclarke.com/EC/WMT.html#Mob> (8 september 2011).
- College Bescherming Persoonsgegevens (2010). *Politiekorpsen handelen in strijd met de wet bij toepassing ANPR*. http://www.cbpweb.nl/Pages/pb_20100128_anpr.aspx (17 december 2010).
- Copp, D. (1999). The Idea of a Legitimate State. *Philosophy & public affairs*. 28 (1): 3-45.
- Crane, N. (2002). *Mercator. The man who mapped the planet*. London: Weidenfeld & Nicolson.
- Crone, G.R. (1978). *Maps and their makers: an introduction to the history of cartography*. Folkestone: Dawson.
- Cuijpers, C.M.K.C. (2011). Slim kiezen bij slimme meters. *Privacy & Informatie*. (3): 131-141.
- De Hert, P.J.A., J. Nouwt, I. Voets en J.G.L. van der Wees (2008). Sms, opsporing en privacy. *Computerrecht*. (4): 154-159.
- De Longueville, B., R.S. Smith en G. Luraschi (2009). "OMG, from here, I can see the flames!": a use case of mining location based social networks to acquire spatio-temporal data on forest fires. *Proceedings of the 2009 International Workshop on Location Based Social Networks*. Seattle, Washington: ACM.

Dobson, J.E. en P.E. Fisher (2003). Geoslavery - Society must contemplate a new form of slavery, characterized by location control. *IEEE technology & society magazine: a publ. of the IEEE Society on Social Implications of Technology*. 22 (1): 47-52.

Dodds, E.R. (1951). *The Greeks and the Irrational*. Berkeley/Los Angeles: University of California Press.

Donk, W.B.H.J. van de en P.W. Tops (1992). Informatisering en democratie: Orwell of Athene? In: Frissen, P.H.A., A.W. Koers en I.T.M. Snellen (red.) *Orwell of Athene? Democratie en informatiesamenleving*. Den Haag: Sdu, 31-74.

Dubbeld, L. (2006). Telemonitoring of cardiac patients: user-centred research as input for surveillance theories. In: Lyon, D. (red.) *Theorizing surveillance: the panopticon and beyond*. Devon: Willan Publishing, 182-205.

Edwards, A.R. (2005). De democratische potentie van internet: democratische intermediaren online. In: Lips, M., V. Bekkers en A. Zuurmond (red.) *ICT en openbaar bestuur*. Utrecht: Lemma, 479-507.

Elk, B. van (2008). Digitaal herkennen, checken en aanhouden. Marechaussee werkt aan systeem voor informatiegestuurd optreden. *NIDV magazine*. (1): 6-10.

Eudes, Y. (2009). Twitter, les pirates et les diplomates. *Le Monde*. http://www.lemonde.fr/technologies/article/2009/08/24/twitter-les-pirates-et-lesdiplomates_1231380_651865.html (6 juni 2012).

European Space Agency (2012). What is Galileo? *ESA - Navigation - the Future - Galileo*. <http://www.esa.int/esaNA/galileo.html> (7 april 2012).

Foucault, M. (1979). Panopticism. From: Discipline and Punish: The Birth of the Prison. In: Webster, F. (red.) *The Information Society Reader*. London: Routledge, 301-312.

Frissen, P.H.A., A.W. Koers en I.T.M. Snellen (1992). *Orwell of Athene? Democratie en informatiesamenleving*. Den Haag: Sdu.

Frissen, P.H.A. (1996). *De virtuele staat. Politiek, bestuur, technologie: een postmodern verhaal*. Schoonhoven: Academic Service.

Frissen, P.H.A. (1999). Voorbij plaats en wezen - De politieke betekenis van virtualisering en deterritorialisering. *Bestuurskunde: orgaan van de Vereniging voor Bestuurskunde*. (5): 189-198.

- Frissen, P.H.A. (2013). *De fatale staat. Over de politiek noodzakelijke verzoening met tragiek*. Amsterdam: Van Genneep.
- Frissen, V., M. van Staden, N. Huijboom, B. Kotterink, S. Huveneers, M. Kuipers en G. Bodea (2008). *Naar een 'User Generated State'? De impact van nieuwe media voor overheid en openbaar bestuur*. Delft: TNO.
- Fuchs, C. (2011). New media, web 2.0 and surveillance. *Sociology Compass*. 5 (2): 134-147.
- Fuchs, C., K. Boersma, A. Albrechtslund en M. Sandoval (red.) (2011). *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. New York: Routledge.
- Gasson, M., M. Meints en K. Warwick (red.) (2005). *FIDIS Deliverable D3.2: A study on PKI and biometrics*. FIDIS Consortium.
- Geser, H. (2004). Towards a Sociological Theory of the Mobile Phone. *Sociology in Switzerland: Sociology of the Mobile Phone. Online Publications (Release 3.0)*. http://socio.ch/mobile/t_geser1.htm (23 augustus 2011).
- Gestel, B. van, L.M. van der Knaap en A. Hendriks (2006). *Toezicht buiten de muren. Een systematische review van extramuraal toezicht op TBS-gestelden en vergelijkbare groepen in het buitenland*. Den Haag: WODC.
- Geuijen, K., P. 't Hart en K. Yesilkagit (2007). Dutch Eurocrats at Work: Getting Things Done in Europe. In: Rhodes, R.a.W., P. 't Hart en M. Noordegraaf (red.) *Observing government elites: up close and personal*. Basingstoke [etc]: Palgrave Macmillan, 131-159.
- Government of South Australia (2006). What is spatial information? *SICOM - About spatial information*. <http://www.environment.sa.gov.au/mapland/sicom/info/index.html> (4 juni 2007).
- Gow, G.A. en M. Ihnat (2004). Prepaid Mobile Phone Service and the Anonymous Caller: Considering Wireless E9-1-1 in Canada. *Surveillance & Society*. 1 (4): 555-572.
- Graaf, L.J. de (2007). *Gedragen beleid. Een bestuurskundig onderzoek naar interactief beleid en draagvlak in de stad Utrecht*. Delft: Eburon.
- Green, N. en S. Smith (2004). 'A Spy in your Pocket?' The Regulation of Mobile Data in the UK. *Surveillance & Society*. 1 (4): 573-587.
- Gunsteren, H. van (1992). *Eigentijds burgerschap*. Den Haag: WRR-publicatie.

Gunsteren, H. van (2008). Burgerschap en veiligheid in Nederland. In: Alberts, G., M. Blankesteyn, B. Broekhans en Y. Van Tilborgh (red.) *Jaarboek Kennissamenleving*. Amsterdam: Aksant, 169-183.

Habermas, J. (1974). The Public Sphere. In: Webster, F. (red.) *The Information Society Reader*. London: Routledge, 350-365.

Haggerty, K. (2006). Tear down the walls: on demolishing the panopticon. In: Lyon, D. (red.) *Theorizing surveillance: the panopticon and beyond*. Devon: Willan Publishing, 23-45.

Haggerty, K. en R. Ericson (2007). The surveillant assemblage. In: Hier, S.P. en J. Greenberg (red.) *The surveillance studies reader*. Maidenhead: Open University Press, 104-116.

Haggerty, K.D. en M. Samatas (red.) (2010). *Surveillance and democracy*. Abingdon: Routledge.

Haverland, M. en D. Yanow (2012). A Hitchhiker's Guide to the Public Administration Research Universe: Surviving Conversations on Methodologies and Methods. *Public Administration Review*. 72 (3): 401-408.

Hendriks, F. (2007). Legitimiteit van bestuur: moeilijkheden en mogelijkheden van gezaghebbend machthebben. In: Cornelissen, E.M.H., P.H.A. Frissen, S. Kensen en T. Brandsen (red.) *Betoverend bestuur: legitimiteit, vitaliteit, meervoudigheid*. Den Haag: Lemma, 63-74.

Hier, S.P. en J. Greenberg (red.) (2007). *The surveillance studies reader*. Maidenhead: Open University Press.

Hildebrandt, M. (2008). Defining Profiling: A New Type of Knowledge? In: Hildebrandt, M. en S. Gutwirth (red.) *Profiling the European citizen: cross-disciplinary perspectives*. Dordrecht: Springer.

Hildebrandt, M. en S. Gutwirth (red.) (2008). *Profiling the European citizen: cross-disciplinary perspectives*. Dordrecht: Springer.

Hill, M. (2009). *The Public Policy Process*. Harlow: Pearson Longman.

Hof, C. van 't, R. van Est en F. Daemen (2010). *Check in / Check uit: de digitalisering van de openbare ruimte*. Rotterdam: NAI Uitgevers.

Hoogwout, M. (2010). *De rationaliteit van de klantgerichte overheid. Een onderzoek naar de spanningen die de invoering van het klantdenken bij gemeenten veroorzaakt en de manier waarop gemeenten daarmee omgaan*. Nieuwegein: Uitgeverij Réunion.

Horjus, S., B. Willemse en A.M. Pot (2010). *Zorgen op afstand. Een pilotstudie naar het effect van GPS voor mensen met beginnende dementie en hun mantelzorgers*. Utrecht: Trimbos-instituut.

Internet Movie Database (2002). *Minority Report*. <http://www.imdb.com/title/tt0181689/> (6 juni 2012).

Isin, E.F. en P.K. Wood (1999). *Citizenship and identity*. London: Sage.

Jin, S. (2013). Recent progresses on Beidou/COMPASS and other global navigation satellite systems (GNSS) –I. *Advances in Space Research*. 51 (6): 941.

Joustra, J.A.S., P. ter Mors en J. Galema (red.) (2005). *Atlas. Geschiedenis, grenzen, conflicten, ideologieën, projecties en vooruitzichten in 168 kaarten*. Amsterdam: Elsevier.

Kaplan, A.M. en M. Haenlein (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*. 53 (1): 59-68.

Keen, A. (2007). *The cult of the amateur: how today's internet is killing our culture*. New York: Doubleday/Currency.

Keymolen, E., B. van den Berg, J.E.J. Prins en V. Frissen (2010). *Vertrouwen in hybride ketens. Een onderzoek in het kader van de Alliantie Vitaal Bestuur*. TNO ICT - Erasmus University Rotterdam - Tilburg University.

Kinneging, A. (2005). *Geografie van goed en kwaad*. Utrecht: Uitgeverij Het Spectrum.

Kool, D. de en J. van Wamelen (2008). De impact van web 2.0 op de kennissamenleving. In: Alberts, G., M. Blankesteyn, B. Broekhans en Y. Van Tilborgh (red.) *Jaarboek Kennissamenleving*. Amsterdam: Aksant, 288-305.

Koops, E.J., R.E. Leenes en P.J.A. De Hert (2008). Grondrechten en nieuwe technologieën. Een rechtsvergelijkend overzicht. *Nederlandsch Juristenblad*. 83 (19): 1157-1164.

Kubben, R. (2007). De nieuwe kleren van de keizer: Tussen sprookjes in het openbaar bestuur en het openbaar bestuur in sprookjes. In: Cornelissen, E.M.H., P.H.A. Frissen, S. Kensen en T. Brandsen (red.) *Betoverend bestuur: legitimiteit, vitaliteit, meervoudigheid*. Den Haag: Lemma, 49-62.

- Küpper, A. (2005). *Location-based Services: Fundamentals and Operation*. Chichester: Wiley.
- Langley, R.B. (2012). GLONASS Fully Operational. *GPS World* 23 (1): 16.
- LCB (2010). *Landelijk Congres der Bestuurskunde 2010: de staat van de privacy*. <http://2010.lcb.nl/> (20 maart 2012).
- Liebrechts, P.T.M.G. (2007). “*Ubi amor, ibi oculus est*”: *Ethiek en literaire vorm in J.M. Coetzee*. Leiden: Universiteit Leiden. http://www.leidenuniv.nl/tekstboekjes/content_docs/oratie_liebrechts.pdf (6 juni 2012).
- Lips, M., V. Bekkers en A. Zuurmond (red.) (2005). *ICT en openbaar bestuur*. Utrecht: Lemma.
- Lipsky, M. (1980). *Street-level Bureaucracy: Dilemmas of the Individual in Public Services*. New York: Russell Sage Foundation.
- Lyon, D. (2001a). *Surveillance society: monitoring everyday life*. Buckingham: Open University Press.
- Lyon, D. (2001b). New directions in theory. From: *Surveillance Society: Monitoring Everyday Life*. In: Webster, F. (red.) *The Information Society Reader*. London: Routledge, 327-344.
- Lyon, D. (red.) (2006a). *Theorizing surveillance: the panopticon and beyond*. Devon: Willan Publishing.
- Lyon, D. (2006b). The search for surveillance theories. In: Lyon, D. (red.) *Theorizing surveillance: the panopticon and beyond*. Devon: Willan Publishing, 3-20.
- Lyon, D. (2007a). *Surveillance studies: an overview*. Cambridge: Polity Press.
- Lyon, D. (2007b). Surveillance, Power, and Everyday Life. In: Mansell, R., C. Avgerou, D. Quah en R. Silverstone (red.) *The Oxford Handbook of Information and Communication Technologies*. New York: Oxford University Press, 449-467.
- Lyon, D. (2010). Identification, surveillance and democracy. In: Haggerty, K.D. en M. Samatas (red.) *Surveillance and democracy*. Abingdon: Routledge, 34-50.
- Mann, S., J. Nolan en B. Wellman (2003). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society*. 1 (3): 331-355.

- Mansell, R., C. Avgerou, D. Quah en R. Silverstone (red.) (2007). *The Oxford Handbook of Information and Communication Technologies*. New York: Oxford University Press.
- Meints, M. en D. Royer (2007). Location information from a technical perspective. In: Cuijpers, C., A. Roosendaal en B.-J. Koops (red.) *D11.5: The legal framework for location-based services in Europe*. FIDIS consortium.
- Michael, M.G., S.J. Fusco en K. Michael (2008). A research note on ethics in the emerging age of überveillance. *Computer communications*. 31 (6): 1192-1199.
- Michiels, F.C.M.A. (2006). *Hoofdzaken van het bestuursrecht*. Deventer: Kluwer.
- Miedema, F. en B. Post (2006). *Evaluatie pilot elektronische volgsystemen*. Nijmegen: ITS-WODC.
- Ministerie van Verkeer en Waterstaat (2007). *Beleidskader benutten*. Den Haag.
- Ministerie van Verkeer en Waterstaat (2009). *Waarom de kilometerprijs?* http://www.verkeerenwaterstaat.nl/onderwerpen/mobiliteit_en_bereikbaarheid/kilometerprijs/waarom_de_kilometerprijs/ (7 juni 2010).
- Mintzberg, H. (1996). Managing Government, Governing Management. *Harvard business review*. 74 (3): 75-83.
- Mitchell, K.J., J. Wolak en D. Finkelhor (2005). Police posing as juveniles online to catch sex offenders: is it working? *Sex Abuse*. 17 (3): 241-67.
- Monmonier, M. (1996). *How to lie with maps*. Chicago: The University of Chicago Press.
- Monmonier, M. (2010). *[No] dig, [no] fly, [no] go: how maps restrict and control*. Chicago: University of Chicago Press.
- Montfort, C. van (2010). Ontwikkelingen in toezicht en verantwoording bij instellingen op afstand. Een terugblik en een blik in de toekomst. *Tijdschrift voor Toezicht*. 1 (1): 6-20.
- Mountain, D. en J. Raper (2001). Positioning techniques for location-based services (LBS): characteristics and limitations of proposed solutions. *ASLIB proceedings*. 53 (10): 404-412.
- Muller, N.J. (2003). *Wireless A to Z*. New York: McGraw-Hill.
- Najbjerg, T. (2012). The Severan Marble Plan of Rome (Forma Urbis Romae). *Stanford Digital Forma Urbis Romae Project*. <http://formaurbis.stanford.edu/docs/FURmap.html> (25 juli 2012).

NDW (2012). Nieuws. Nieuwe masten om verkeersdrukte te meten. http://www.ndw.nu/nieuws/bekijk/94/nieuwe_masten_om_verkeersdrukte_te_meten (18 juli 2013).

NOAA (2012). Space Segment. *GPS.gov: Official U.S. Government information about the Global Positioning System (GPS) and related topics*. <http://www.gps.gov/systems/gps/space/> (8 april 2012).

Nouwte, J. (2008). Reasonable expectations of geo-privacy? *SCRIPTed*. 5 (2): 375-403.

Nouwte, J. en J.G.L. van der Wees (2008). *Juridische aspecten van geo-informatie*. Alliantie Vitale Bestuur/Universiteit van Tilburg.

NRC Handelsblad (2010). Gezichtsherkenning tegen raddraaiers trams Rotterdam. http://www.nrc.nl/binnenland/article2553198.ece/Gezichtsherkenning_tegen_raddraaiers_trams_Rotterdam (9 juni 2010).

NS (2010). Reisregels en bescherming persoonsgegevens. <http://www.ns.nl/cs/Satellite/reizigers/ov-chipkaart/reisregels-en-bescherming> (31 augustus 2010).

Nu.nl (2006). Politie blij met resultaat sms-bom Sévère. *Nu.nl/internet*. <http://www.nu.nl/news.jsp?n=697945&c=50&rss> (22 augustus 2011)

Nu.nl (2011). Chinees navigatienetwerk Beidou operationeel. *Nu.nl/internet*. <http://www.nu.nl/internet/2702155/chinees-navigatienetwerk-beidou-operationeel.html> (7 april 2012).

Onsrud, H.J. (2008). Implementing Geographic Information Technologies Ethically. *ArcNews*. <http://www.esri.com/news/arcnews/fall08articles/implementing-gi-technologies.html> (22 augustus 2011).

Ooijen, C.W.van en S.B. Soeparman (2010). Toezicht in de voorzorgstaat: kennis en informatiegebruik tussen staatscontrole en sociabiliteit. In: Pieter, W., F.K. Boersma, G. Albers, J. Timmer, A. Dijkstra en M. Popkema (red.) *Inzicht en toezicht: controle in de kennissamenleving*. Amsterdam: Uitgeverij Aksant, 161-181.

Ooijen, C.W. van (2011). Legitimacy Issues Regarding Citizen Surveillance: The Case of ANPR Technology in Dutch Policing. In: Van der Hof, S. en M.M. Groothuis (red.) *Innovating Government*. Den Haag: T.M.C. Asser Press, 197-216.

Ooijen, C.W. van en A.M. Bokhorst (2012). Securing the Legitimacy of Surveillance. Automatic Number Plate Recognition in Dutch policing. In: Vande Walle, G., E. Van Den Herrewegen en N. Zurawski (red.) *Crime, Security and Surveillance. Effects for the Surveillant and the Surveilled*. The Hague: Eleven International Publishing, 123-144.

Openbaar ministerie (2014). *TBS*. <http://www.om.nl/onderwerpen/tbs/> (8 juni 2014).

Ordnance Survey (2007). *An introduction to Ordnance Survey. Ordnance Survey - Great Britain's national mapping agency*. <http://www.ordnancesurvey.co.uk/oswebsite/media/features/introos/index.html> (27 juni 2007).

Orwell, G. (1949). *1984*. New York: New American Library.

Osimo, D. (2008). *Web 2.0 in government: Why and how?* Seville (Spain): Joint Research Centre (JRC) - Institute for Prospective Technological Studies (IPTS).

Oxford University Press (2008). Compact Oxford English Dictionary. *AskOxford*. http://www.askoxford.com/concise_oed/territory?view=uk (6 februari 2008).

Pel, B. (2012). *System Innovation as Synchronization; innovation attempts in the Dutch traffic management field*. Rotterdam: Erasmus University.

Pieterman, R., J.C. Hanekamp en L. Bergkamp (2006). Onzekere voorzorg bedreigt rechtszekerheid. *Nederlandsch Juristenblad*. (1): 2-8.

Pieterman, R. (2008). *De voorzorgcultuur: streven naar veiligheid in een wereld vol risico en onzekerheid*. Den Haag: Boom Juridische uitgevers.

Poel, X. van de (2001). Wereldbeelden tot de tijd van Mercator. In: Depuydt, F. en M. Goossens (red.) *Van Mercator tot computerkaart. Een geschiedenis van de cartografie*. Turnhout: Brepols Publishers,

Politie en VNG (2013). *Burgernet. Samen voor een veilige buurt*. <https://www.burgernet.nl> (17 november 2013).

Politie Rotterdam-Rijnmond, Korps Landelijke Politiediensten en VtS Politie Nederland, onderdeel NPI, (2008). *Automatic Number Plate Recognition, Naar een landelijke toepassing. Visiedocument ANPR*.

Pontier, J.-M. (1997). Territorialisation et déterritorialisation de l'action publique. *L'actualité juridique*. 53 (10): 723 - 730.

Poster, M. (1990). *Mode of information: Poststructuralism and social context*. Cambridge: Polity Press.

Provincie Noord-Brabant (2010). *Website actuele verkeersinformatie*. <http://brabant.nl/dossiers/dossiers-op-thema/verkeer-en-vervoer/innovatie-en-verkeer/Actuele-verkeersinformatie.aspx> (11 juni 2010).

Raad van Hoofdcommissarissen (2005). *Politie in ontwikkeling. Visie op de politiefunctie*. Den Haag: NPI.

Raper, J., G. Gartner, H. Karimi en C. Rizos (2007). A critical evaluation of location based services and their potential. *Journal of Location Based Services*. 1 (1): 5-45.

Rijksoverheid (2010). *Vrijheid en verantwoordelijkheid. Regeerakkoord VVD - CDA*. <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/09/30/regeerakkoord-vvd-cda.html> (15 augustus 2011).

Rijksoverheid (2012a). *Wat is rode diesel en wie mag hier gebruik van maken?* <http://www.rijksoverheid.nl/onderwerpen/btw-en-accijns/vraag-en-antwoord/wat-is-rode-diesel-en-wie-mag-hier-gebruik-van-maken.html> (22 oktober 2012).

Rijksoverheid (2012b). *Bruggen slaan. Regeerakkoord VVD - PvdA*. <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/10/29/regeerakkoord.html> (15 november 2013).

Rijksoverheid (2013a). *Nederlandse nationaliteit*. <http://www.rijksoverheid.nl/onderwerpen/nederlandse-nationaliteit/nederlander-worden> (9 september 2013).

Rijksoverheid (2013b). *Wetsvoorstel over het vastleggen van kentekens naar Tweede Kamer*. <http://www.rijksoverheid.nl/nieuws/2013/02/12/wetsvoorstel-over-het-vastleggen-van-kentekens-naar-tweede-kamer.html> (26 juni 2013).

Sassen, S. (2007). Electronic networks, power & democracy. In: Mansell, R., C. Avgerou, D. Quah en R. Silverstone (red.) *The Oxford Handbook of Information and Communication Technologies*. New York: Oxford University Press, 339-361.

Scott, J.C. (1998). *Seeing like a state. How certain schemes to improve the human condition have failed*. New Haven, CT [etc.]: Yale University Press.

Smits, J.M. (2008). Je plaats kennen! Kan het recht dat plaatsen? *Privacy & Informatie*. 11 (1): 2-9.

- Snellen, I.T.M. (2000). Territorialising governance and the state: Policy dimensions of Geographic Information Systems. *Information infrastructure and policy: an international journal on the development, adoption, use and effects of information technology*. 6 (3): 131-138.
- Snellen, I.T.M. (2005). E-government: a challenge for public management. In: Ferlie, E., L.E. Lynn en C. Pollitt (red.) *The Oxford Handbook of Public Management*. New York: Oxford University Press, 398-421.
- Soenens, E. (2006). Conceptual and sociological issues of Mobility and Identity. In: Royer, D. (red.) *FIDIS Deliverable D11.1: Collection of Topics and Clusters of Mobility and Identity - Towards a Taxonomy of Mobility and Identity*. FIDIS Consortium, 29-40.
- Sparks, R.F., A. Bottoms en W. Hay (1996). *Prisons and the problem of order*. Oxford: Clarendon Press.
- Stevens, M. en J. de Jong (2010). 'I always feel like somebody's watching me'. Van surveillance naar coveillance. In: Pieter, W., F.K. Boersma, G. Albers, J. Timmer, A. Dijkstra en M. Popkema (red.) *Inzicht en toezicht: controle in de kennissamenleving*. Amsterdam: Uitgeverij Aksant, 149-160.
- Surowiecki, J. (2004). *The wisdom of crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies, societies, and nations*. London: Little, Brown.
- Taylor, J.A., A.M.B. Lips en J. Organ (2009). Identification Practices in Government: Citizen Surveillance and the Quest for Public Service Improvement. *Identity in the Information Society*. 1 (1).
- Tops, P.W. en S. Zouridis (2000). *Burgers en overheidscommunicatie*. Document vervaardigd ten behoeve van de commissie Toekomst Overheidscommunicatie. Centrum voor recht, bestuur en informatisering, Katholieke Universiteit Brabant.
- Torpey, J. (2000). *The invention of the passport: surveillance, citizenship and the state*. Cambridge: Cambridge University Press.
- Torpey, J. (2007). Coming and going: on the state monopolization of the legitimate 'means of movement'. In: Hier, S.P. en J. Greenberg (red.) *The surveillance studies reader*. Maidenhead: Open University Press, 52-66.
- Trommel, W. (2009). *Gulzig bestuur*. Den Haag: Lemma.

Tweede Kamer der Staten-Generaal (2009). Regels voor het in rekening brengen van een gebruiksafhankelijke prijs voor het rijden met een motorrijtuig (Wet kilometerprijs). *Kamerstukken II 2009/10. 32 216. nr. 2.*

Vanneste, D. (2001). Geografische informatiesystemen. In: Depuydt, F. en M. Goossens (red.) *Van Mercator tot computerkaart. Een geschiedenis van de cartografie.* Turnhout: Brepols Publishers,

Vedder, A. (2007a). Towards a defensible conceptualization of the legitimacy of NGOs. In: Vedder, A. (red.) *NGO involvement in international governance and policy: sources of legitimacy.* Leiden: Nijhoff, 197-212.

Vedder, A. (2007b). *NGO involvement in international governance and policy: sources of legitimacy.* Leiden [etc.]: Nijhoff.

Vedder, A. (2007c). Questioning the legitimacy of non-governmental organizations. In: Vedder, A. (red.) *NGO involvement in international governance and policy: sources of legitimacy.* Leiden [etc.]: Nijhoff, 1-20.

Vedder, A., L.J.G. van der Wees, E.J. Koops en P.J.A. De Hert (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.* Den Haag: Rathenau Instituut.

Vonk, G., S. Geertman en P. Schot (2007). New Technologies Stuck in Old Hierarchies: The Diffusion of Geo-Information Technologies in Dutch Public Organizations. *Public administration review.* 67 (4): 745-756.

Wilmink, I., B. Immers en H. Schuurman (2011). *Toepassingsmogelijkheden van coöperatieve systemen en services in Nederland.* <http://www.verkeerskunde.nl/Uploads/2011/11/Bijdrage51.pdf> (17 november 2013).

Wood, D. (1993). *The power of maps.* London: Routledge.

WRR, Wetenschappelijke Raad voor het Regeringsbeleid (1998). *Staat zonder land: een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie* Den Haag: Sdu Uitgevers.

WRR, Wetenschappelijke Raad voor het Regeringsbeleid (2008). *Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid.* Amsterdam: Amsterdam University Press.

Yanow, D. (2007). Interpretation in Policy Analysis: On Methods and Practice. *Critical Policy Analysis.* 1 (1): 109-121.

Zouridis, S. (2007). De legitimiteit van recht en bestuur: signalen voor legitimiteitserosie geanalyseerd. In: Cornelissen, E.M.H., P.H.A. Frissen, S. Kensen en T. Brandsen (red.) *Betoverend bestuur: legitimiteit, vitaliteit, meervoudigheid*. Den Haag: Lemma, 93-116.

Zouridis, S. (2009). *De dynamiek van bestuur en recht: over de rechtsstaat als bestuurswetenschappelijk fenomeen*. Den Haag: Lemma.

Zurawski, N. (2007). Einleitung: Surveillance Studies: Perspektiven eines Forschungsfeldes. In: Zurawski, N. (red.) *Surveillance Studies. Perspektiven eines Forschungsfeldes*. Opladen & Farmington Hills: Barbara Budrich, 7-24.

Zuurmond, A. (1994). *De infocratie: een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk*. Den Haag: Phaedrus.

ENGLISH SUMMARY

The risk of the mobile citizen. Public mobility surveillance for information about citizens' whereabouts.

Mobile citizens attract the attention of government in various policy domains, such as traffic management, tourism, emergency services and policing. Government increasingly uses surveillance technologies, like GPS and mobile phones to collect mobility data about citizens, in order to monitor and control this mobility.

In this study, I have introduced the concept of **public mobility surveillance** to study this domain of government activities. At the outset of this research, I have defined public mobility surveillance as:

The digital collection and processing of mobility data about persons, whether identifiable or not, in order to influence or manage for public purposes those whose data have been gathered.

I have argued that both the academic and the societal debate are somewhat polemic, and lack substantial insight into the practice of public mobility surveillance. The goal of this research has been twofold. The first goal is to gather insight into how the meaning of public mobility surveillance is construed in public policy in order to assess in what way technological possibilities and limitations have an effect on policy practice. The second goal is to develop a conceptual framework to understand the implications of public mobility surveillance for the government-citizen relationship from a policy perspective. Correspondingly, the main research question is:

What are the implications of public mobility surveillance for the way in which government shapes its relationship with citizens?

The main question has been divided into five sub-questions.

1 - What is public mobility surveillance from an ICT-perspective?

This first sub-question entails the mapping of the characteristics of information and communication technologies that can be used for public mobility surveillance. The aim of such mapping is twofold, first, to contribute to a theoretical foundation of the concept and, second, to facilitate the description of practices of public mobility

surveillance. From an ICT-perspective, public mobility surveillance entails gathering, connecting and analysing data about spatial mobility.

The essence of mobility is the *ability* of an object to move in the dimensions of space and time. Consequently, public mobility surveillance refers to both non-moving and moving people. Whether people are moving, and if so, where and when, is information which is typically obtained by means of public mobility surveillance. Mobility consists of two dimensions: the (possibly) moving object of surveillance and the movement itself. Consequently, three categories of mobility data have been distinguished: object data, location data and time data.

Data about the object of surveillance help answer the question: ‘What is moving?’ Three answering categories have been distinguished: artefacts (e.g. mobile phones), bodies (e.g. Mister X or a group of men), and actions (e.g. potential burglars). Data about the movement itself consist of location data (space) and temporal data (time). The categories of spatial, network and descriptive locations help to express movement in the dimension of space: ‘Where is someone moving?’ Time can be understood in terms of information about the past, present or future: ‘When is someone moving?’ Table 1 summarises the categories of mobility data.

Mobility data can be gathered by means of several location technologies: satellite systems, networking technology, other wireless technologies, sensor systems, chip card systems and hybrid technology. Geographic Information Systems (GIS) serve to manage, visualise and interpret mobility data against the background of geo-information. Several actors are connected in the information chain of gathering, connecting and analysing mobility data: the object of surveillance, the content provider, the information provider and the end user. When considering the roles government and citizens can fulfil, it turns out that both of them can sometimes have several information roles at the same time.

MOBILITY CATEGORY	MANIFESTATION	EXAMPLES
<i>Object</i>		
Artefact	Device data	SIM-card number; chip card number
Body	(Aggregated) personal data	Name; age; gender
Action	Situational identity	Car driver; victim; witness
<i>Location</i>		
Spatial	Coordinates	Point in a Cartesian (X,Y,Z) or ellipsoid (N; E) coordinate system
Network	Cell-topology	IP address; place in a GSM network
Descriptive	Geographical reference	Address; name of building/park/city
<i>Time</i>		
Present	Data gathered in real time	Current location of fugitive wearing GPS ankle bracelet; location of 112 emergency call
Past	Saved data	Historic traffic data; public transport chip card journey time data
Future	Calculated data	Expected traffic jam; Terrorism threat

Table 1: Mobility data

2 - What is the political-administrative background of public mobility surveillance?

I have argued that it doesn't suffice to look at ICT-characteristics to understand the meaning of public mobility surveillance. Study of existing literature reveals that information about mobility was already of great strategic importance to states before the rise of ICTs.

From a political-administrative point of view, public mobility surveillance is the result of two developments. On the one hand it is a continuation of activities deployed by emerging European nation states in the seventeenth and eighteenth centuries: state cartography and the implementation of the instrument of national passport. A connection is revealed between controlling people's mobility and defining and guarding territorial boundaries. Ever since the rise of states, governments have been concerned with defining their territories, protecting existing resources and attracting new ones. As such, from a historical point of view it is essential for the self-preservation of the state to know where the increasingly mobile citizens and non-citizens are and to control where they can and cannot go. Public mobility surveillance can be considered as a modern variation of the passport but with more technological possibilities and more applications in domains of public policy.

On the other hand, public mobility surveillance is an acceleration of these traditional state activities as a result of the twentieth century threats to the territorial basis of the state: increased mobility and the ICT revolution. Therefore, paradoxically, public mobility surveillance can be understood as a reaction to characteristics of the ICT revolution it is part of.

3 - Which perspectives on surveillance in the government-citizen relationship can be distinguished?

This sub-question addresses the second part of the main research question, *implications for the way in which government shapes its relationship with citizens*, in a theoretical way.

What could these implications involve? In order to answer this question, I've linked up three perspectives on surveillance (control, interaction and precaution) to a threefold conceptualisation of the government-citizen relationship (ruler - subject, service provider - client, and democratic institution - citizen). Each of these surveillance perspectives contains both assumptions about technology (policy possibilities) and legitimacy (evaluation criteria in terms of legality, normative justification and social acceptability). These three surveillance perspectives reveal different logics behind surveillance activities in the government-citizen relationship. Consequently, the

perspectives have different theoretical implications for the way in which the government-citizen relationship is shaped.

The control perspective on surveillance focuses on the question how panoptic surveillance, which controls and disciplines citizens, can be legitimised while protecting citizens' privacy at the same time. The interaction perspective presents surveillance as a connection between different actors in society. Consequently, from this perspective the question is posed how access to surveillance systems and the value and quality of the produced information can be legitimised. The precautionary perspective supposes that surveillance technology can serve to identify and control risks. The legitimacy concern in this perspective is the evaluation of the grounds for defining risks and categories of citizens. Table 2 shows the theoretical framework of implications of surveillance for the government-citizen relationship.

	GOVERNMENT - CITIZEN RELATIONSHIP		
SURVEILLANCE PERSPECTIVE	<i>Ruler - Subject</i>	<i>Service provider - Client</i>	<i>Democratic institution - Citoyen</i>
<i>Control</i> <i>Power and privacy</i>	Surveillance facilitates and replaces government enforcement of regulation.	Based on surveillance data about citizens, government facilitates access to public services.	By means of sousveillance ⁷¹ citizens ensure transparency of government surveillance.
	Panoptic discipline ensures that citizens comply with government rules and regulation.	All citizens become reactive or passive clients.	Sousveillance stimulates government to account for surveillance of citizens.
<i>Interaction</i> <i>Free access to surveillance and quality of information</i>	Government regulation and enforcement are supplemented by civic norms and enforcement.	Government becomes a passive, moderating and reactive service provider.	Surveillance facilitates self- governance and cooperation with the government.
	Government and citizens stimulate fellow citizens to participate in enforcement.	As prosumers of surveillance information citizens to a large extent replace public service provision by the government.	Citizens demand an active role in the enforcement of fellow citizens.
<i>Precaution</i> <i>Defining risks and (groups of) risk citizens</i>	Government regulation and enforcement change quickly and focus on risk groups.	Dependent on group characteristics government selectively and proactively provides services to citizens.	Risk analyses have a central position in the accounting for policy choices.
	As a result of limited knowledge about changing norms, citizens find themselves in a Kafkaesque uncertainty.	Particular groups of citizens become reactive or passive clients.	Risks on the public agenda easily reach the government's surveillance agenda.

Table 2: Surveillance perspectives and the government-citizen relationship

⁷¹ The term sousveillance was introduced by Steve Mann and points to inverse surveillance: 'One way to challenge and problematize both surveillance and acquiescence to it is to resituate these technologies of control on individuals, offering panoptic technologies to help them observe those in authority' (Mann, Nolan en Wellman, 2003: 332).

4 - To what extent do the different surveillance perspectives manifest themselves in the policy practice of public mobility surveillance?

In order to answer this sub-question I have conducted two empirical case studies into two policy practices of public mobility surveillance. Both case studies concern public executive agencies in the Netherlands. The first case study focuses on the application of automatic number plate recognition (ANPR) by one of the Dutch regional police forces. The second case study involves innovation in the collection and processing of mobility data by the National Data Warehouse (NDW), which is part of *Rijkswaterstaat*, the Dutch executive agency for infrastructure and mobility policy.

Methodologically, this study can be characterised as an interpretive-qualitative policy analysis. I have analysed how policy actors interpret technological possibilities and legitimacy issues concerning public mobility surveillance. Data generating methods included observation of interactions during meetings and outside the office, interviews with stakeholders and document study (policy documents; internal and external correspondence).

The results of the empirical study show that technology and legitimacy assumptions from all three surveillance perspectives can be found in the practice of public mobility surveillance. However, the theoretical assumptions manifested themselves in varying extent. Table 3 summarises the extent to which the technology and legitimacy assumptions pertaining to the three surveillance perspectives of control, interaction and precaution were found in each of the two cases studies. Consequently, insight is gained into assumptions that influence decision-making about technology involved in public mobility surveillance.

The assumptions about technology and legitimacy of public mobility surveillance as found in the two policy practices have important implications for the way in which government shapes its relationship with citizens.

TECHNOLOGY AND LEGITIMACY ASSUMPTIONS	ANPR - POLICE	INNOVATION - NDW
Control		
Widespread control of citizens (technology assumption)	Strong	None
Disciplining of citizens (technology assumption)	None	None
Usage of surveillance versus citizens (legitimacy assumption)	Strong	Strong
Protecting citizens' privacy (legitimacy assumption)	Strong	Weak
Interaction		
Connecting government and citizens (technology assumption)	None	None
Joint creation of information (technology assumption)	None	None
Access to surveillance information (legitimacy assumption)	Weak	Strong
Relevance and quality of surveillance information (legitimacy assumption)	Weak	Strong
Precaution		
Identifying risks and risk citizens (technology assumption)	Weak	Weak
Containing risks (technology assumption)	Strong	Strong
Defining risks and categories of risk citizens (legitimacy assumption)	Weak	None

Table 3: Empirical manifestation of surveillance perspectives

5 - How is the government-citizen relationship shaped as a result of the characteristics of the surveillance perspectives found in the policy practices?

Based on the theoretical and empirical results, I have drawn five conclusions and one overall conclusion.

1. There's a limited connection between technology and legitimacy assumptions.
2. The precautionary and interaction perspectives are on the rise.
3. The mobile subject is increasingly approached as a risk.
4. Government strives for imperceptible service to clients and protection against risks.
5. Provision of information to the citizen is limited.

Overall conclusion: the mobile citizen as a risk

In all three dimensions of the government-citizen relationship mobile citizens are predominantly considered as potential causes of disasters and discomfort. Public mobility surveillance is aimed at evaluating the mobile citizen in terms of a risk to society. It facilitates the government in assessing which mobile subjects could disobey norms and rules, and therefore pose a potential threat to society. Mobile clients are evaluated in terms of risks as well, and benefit from imperceptible services when the surveillance system doesn't label them as a risk. There is also a dominant risk perception when addressing mobile citizens. They receive little information about government activities related to public mobility surveillance because their surveillance poses a risk to the continuation of those activities.

The government defines risks based not only on the object characteristics of citizens, but increasingly on past and present data about citizens' movements. The analysis of citizens' movement characteristics may cause certain locations to be marked as (temporary) risk locations.

By approaching citizens and their movements as risks to society, government displays a particular interpretation of the precautionary perspective. Precaution is predominantly aimed at mobile citizens posing risks, rather than those being at risk. Protecting mobile citizens against potential risks *en route* is not the primary aim of public mobility surveillance. It is rather focused on the damage a mobile citizen may pose to state and society.

RÉSUMÉ FRANÇAIS

Le risque du citoyen mobile. Surveillance publique de la mobilité du citoyen: où il est, où il va.

Le citoyen mobile est l'objet de toutes les attentions des gouvernements dans divers domaines politiques, tels que la gestion du trafic routier, le tourisme, les services d'urgence et la police. Les gouvernements utilisent de plus en plus les technologies de surveillance, tels que le GPS et les téléphones portables, pour recueillir des données sur la mobilité des citoyens, et ce afin de surveiller et contrôler cette mobilité.

Dans cette thèse, j'ai introduit le concept de la **surveillance publique de la mobilité** afin d'étudier ce domaine d'activité gouvernementale. Au début de cette étude, j'ai défini la notion de la surveillance publique de la mobilité de la manière suivante:

La collecte numérique et le traitement de données de mobilité des personnes, qu'elles soient identifiables ou non, dans le but d'influencer ou de contrôler à des fins publiques celles dont les données ont été recueillies.

J'ai argumenté que le débat, tant scientifique que social, est quelque peu polémique, et est marqué par le manque de renseignements substantiels sur la pratique de la surveillance publique de la mobilité. Le but de cette étude est double. Le premier objectif est de disposer d'un aperçu de la façon dont la surveillance publique de la mobilité est interprétée dans les politiques publiques afin d'évaluer dans quelle mesure les possibilités et les limites technologiques ont un effet sur la prise de décision. Le deuxième objectif est de développer un cadre conceptuel afin de comprendre, du point de vue de l'administration publique, les implications de la surveillance publique de la mobilité sur la relation entre le gouvernement et les citoyens. Par conséquent, la question de recherche principale est la suivante:

<p>Quelles sont les implications de la surveillance publique de la mobilité sur la manière dont le gouvernement façonne sa relation avec les citoyens?</p>

La question principale a été divisée en cinq sous-questions.

1 – Qu'est-ce que la surveillance publique de la mobilité d'un point de vue technologique?

Cette première sous-question amène à décrire les caractéristiques des technologies de l'information et de la communication qui peuvent être utilisées pour la surveillance publique de la mobilité. L'objectif de cette description est double, d'abord, elle permet de contribuer à une fondation théorique du concept et, d'autre part, de faciliter la description des pratiques de surveillance publique de la mobilité. D'un point de vue technologique, la surveillance publique de la mobilité entraîne la collecte, la mise en relation et l'analyse des données de la mobilité spatiale.

L'essence de la mobilité est *la capacité* d'un objet à se déplacer dans les dimensions de l'espace et du temps. Par conséquent, la surveillance de la mobilité publique désigne à la fois le non-mouvement et le mouvement des personnes. Le fait que les gens soient en mouvement, et dans l'affirmative, où et quand se déplacent-ils, sont des informations typiquement obtenues par la surveillance publique de la mobilité. La mobilité se compose de deux éléments: l'objet mobile surveillé et son mouvement lui-même. Par conséquent, trois catégories de données de mobilité ont été identifiées: les données de l'objet, les données de localisation et les données de temps.

Les données sur l'objet de la surveillance aident à répondre à la question: 'Qui / qu'est-ce qui se déplace?' Trois catégories de réponses ont été distinguées: les artefacts (par exemple, les téléphones mobiles), les corps (par exemple, Monsieur X ou un groupe d'individus de sexe masculin), et les actions (par exemple, les cambrioleurs potentiels). Les données sur le mouvement lui-même se composent de données de localisation (espace) et de données temporelles (temps). Les catégories de lieux spatiaux, réseaux et descriptifs servent à exprimer le mouvement dans la dimension d'espace: 'Où est-ce que quelqu'un se déplace?'. Le temps concerne de l'information sur le passé, le présent ou le futur: 'Quand est-ce que quelqu'un se déplace?'. Le tableau 1 résume la typologie des données sur la mobilité.

Les données sur la mobilité peuvent être recueillies par le biais de plusieurs types de technologies de localisation: les systèmes de satellites, les technologies de mise en réseau, les autres technologies sans fil, les systèmes de capteurs, les systèmes de cartes à puce et les technologies hybrides. Les systèmes d'information géographique (SIG) servent à gérer, visualiser et interpréter les données de mobilité dans le contexte de la géo-information. Plusieurs acteurs sont impliqués dans la chaîne informationnelle de la collecte, la connexion et l'analyse des données de mobilité: l'objet de la surveillance, le fournisseur de contenu, le fournisseur d'informations et l'utilisateur final. Lorsque l'on examine les rôles que le gouvernement et les citoyens peuvent avoir, il s'avère que tous les deux peuvent parfois en avoir plusieurs en même temps.

CATÉGORIE DE MOBILITÉ	MANIFESTATION	EXEMPLES
Objet		
Artefact	Données d'appareil	Numéro de carte à puce
Corps	Données personnelles (agrégats)	Nom; âge; sexe
Action	Identité de la situation	Conducteur; victime; témoin
Lieu		
Spatial	Coordonnées	Point dans un système de coordonnées Cartésiennes (X,Y,Z) ou ellipsoïdales (N; E)
Réseau	Topologie cellulaire	Adresse IP; lieu dans un réseau GSM
Descriptif	Référence géographique	Adresse; nom de bâtiment/parc/ville
Temps		
Présent	Données recueillies en temps réel	Localisation des fugitifs portant un bracelet électronique GPS aux chevilles; lieu d'un appel d'urgence
Passé	Données sauvegardées	Données historiques de trafic; données de voyage du pass Navigo
Futur	Données calculées	Embouteillage prévu; Menace de terrorisme

Tableau 1: Données de mobilité

2 – Quelles sont les origines politiques et administratives de la surveillance publique de la mobilité?

J'ai fait valoir qu'il ne suffit pas de regarder les caractéristiques technologiques pour comprendre le sens de la surveillance publique de la mobilité. Une étude de la littérature existante révèle que l'information sur la mobilité était déjà d'une importance stratégique pour les états bien avant l'avènement des technologies de l'information et de la communication (TIC).

D'un point de vue politique et administratif, la surveillance publique de la mobilité est le résultat de deux évolutions. D'une part, il s'agit d'un prolongement des activités déployées par les États-nations européens émergents aux XVII^e et XVIII^e siècles: la cartographie de l'état et la mise en œuvre de l'instrument de passeport national. Un lien apparaît entre le contrôle de la mobilité des personnes, d'une part et la définition et la garde des frontières du territoire, d'autre part. Depuis la naissance des États, les gouvernements ont toujours été préoccupés par la définition de leurs territoires, la protection des ressources existantes ainsi que l'acquisition de nouvelles ressources. En tant que tel, d'un point de vue historique, il est essentiel pour l'auto-préservation de l'État de savoir où les citoyens et les non-citoyens, de plus en plus mobiles, se trouvent et de contrôler où ils peuvent et ne peuvent pas aller. La surveillance publique de la mobilité peut être considérée comme une variation moderne du passeport, mais avec plus de possibilités technologiques et plus d'applications dans les domaines de la politique publique.

D'autre part, la surveillance publique de la mobilité est une accélération des activités étatiques traditionnelles à la suite des menaces à l'encontre de la base territoriale de l'Etat au XX^e siècle: la mobilité accrue et la révolution des TIC. Par conséquent, et paradoxalement, la surveillance publique de la mobilité peut être considérée comme une réaction à certaines caractéristiques de la révolution des TIC, dont elle fait partie.

3 – Quelles perspectives sur la surveillance dans la relation entre le gouvernement et les citoyens peuvent être distinguées?

Cette sous-question porte sur la deuxième partie de la question de recherche principale, *les implications sur la manière dont le gouvernement façonne sa relation avec les citoyens*, d'une manière théorique.

En quoi pourraient consister ces implications? Afin de répondre à cette question, j'ai analysé trois perspectives de surveillance (contrôle, interaction et précaution) en lien avec une triple conceptualisation de la relation entre le gouvernement et les citoyens

(dominateur - sujet, prestataire de services - client, et institution démocratique - coproducteur). Chacune de ces perspectives de surveillance se caractérise par des présomptions relatives à la technologie (possibilités politiques) et des présomptions relatives à la légitimité (critères d'évaluation en termes de légalité, justification normative et l'acceptation sociale). Ces trois perspectives de surveillance révèlent des logiques différentes derrière les activités de surveillance dans la relation entre le gouvernement et les citoyens. Par conséquent, les perspectives ont des implications théoriques différentes sur la manière dont se noue la relation entre le gouvernement et les citoyens.

La perspective de contrôle se concentre sur la question de savoir comment la surveillance panoptique, qui contrôle et discipline les citoyens, peut être légitimée tout en protégeant la vie privée des citoyens. Dans une perspective d'interaction la surveillance se présente comme une connexion entre les différents acteurs de la société. De ce point de vue, la question de la légitimation de l'accès aux systèmes de surveillance, ainsi que de la valeur et de la qualité de l'information produite, se pose. Dans une perspective de précaution, on suppose que la technologie de surveillance peut servir à identifier et maîtriser les risques. De ce point de vue, le souci de légitimité est l'évaluation des motifs pour définir les risques et les catégories de citoyens. Le tableau 2[présente le cadre théorique d'implications de la surveillance dans la relation entre le gouvernement et les citoyens.

PERSPECTIVE DE SURVEILLANCE	RELATION GOUVERNEMENT - CITOYEN		
	<i>Dominateur - Sujet</i>	<i>Prestataire de services - Client</i>	<i>Institution démocratique - Coproducteur</i>
Contrôle <i>Pouvoir et vie privée</i>	La surveillance facilite et remplace l'application gouvernementale de la réglementation.	Basé sur des données de surveillance sur les citoyens, le gouvernement facilite l'accès aux services publics.	Par le biais de sousveillance, ⁷² les citoyens assurent la transparence de la surveillance par le gouvernement.
	La discipline panoptique assure que les citoyens se conforment aux règles et à la réglementation publique.	Tous les citoyens deviennent des clients réactifs ou passifs	La sousveillance stimule le gouvernement à rendre compte de sa surveillance des citoyens.
Interaction <i>Accès libre à la surveillance et qualité d'informations</i>	La réglementation gouvernementale et sa mise en œuvre sont complétées par des normes et mises en œuvre civiques.	Le gouvernement devient passif, modérateur et réactif en fournissant des services aux citoyens.	La surveillance facilite l'auto-gouvernance et la coopération avec le gouvernement.
	Le gouvernement et les citoyens encouragent d'autres citoyens à participer à la mise en œuvre des règles.	Comme prosommateurs de l'information de surveillance, les citoyens remplacent les prestations de services publics du gouvernement dans une large mesure.	Les citoyens souhaitent jouer un rôle actif dans la mise en œuvre des normes envers leurs concitoyens.

⁷² Le terme 'sousveillance' a été introduit par Steve Mann et indique la surveillance inverse: 'One way to challenge and problematize both surveillance and acquiescence to it is to resituate these technologies of control on individuals, offering panoptic technologies to help them observe those in authority' (Mann, Nolan en Wellman, 2003: 332).

PERSPECTIVE DE SURVEILLANCE	<i>Dominateur - Sujet</i>	<i>Prestataire de services - Client</i>	<i>Institution démocratique - Coproducteur</i>
<i>Précaution</i> <i>Définition des risques et (groupes de) citoyens à risque</i>	La réglementation gouvernementale et son application changent rapidement et se concentrent sur les groupes à risque.	Le gouvernement fournit des services sélectifs et proactifs aux citoyens dépendant des caractéristiques de groupe.	L'analyse des risques occupe une position centrale dans la justification des choix politiques.
	Suite à des connaissances limitées sur l'évolution des normes, les citoyens se trouvent dans une incertitude kafkaïenne.	Des groupes particuliers de citoyens deviennent des clients réactifs ou passifs.	Les risques sur l'agenda public atteignent facilement le programme de surveillance du gouvernement.

Tableau 2: Perspectives de surveillance dans la relation gouvernement-citoyen

4 - Dans quelle mesure les différentes perspectives de surveillance se manifestent dans la pratique de la surveillance publique de la mobilité?

Afin de répondre à cette sous-question, j'ai réalisé deux études de cas empiriques dans deux pratiques de la surveillance publique de la mobilité. Ces études ont été effectuées auprès d'agences exécutives publiques aux Pays-Bas. La première étude de cas porte sur la mise en œuvre des systèmes de reconnaissance automatique de plaques d'immatriculation (ANPR) par la police d'une région néerlandaise. La deuxième étude de cas concerne l'innovation dans la collecte et le traitement de données de mobilité par la banque de données nationale (NDW) qui fait partie du *Rijkswaterstaat*, l'organisme exécutif néerlandais pour les infrastructures et la mobilité.

Sur le plan méthodologique, ces études peuvent être considérées comme des analyses de la politique interprétative et qualitative. J'ai analysé la façon dont les acteurs publics interprètent les possibilités technologiques et la question de la légitimité concernant la surveillance publique de la mobilité. Les méthodes de collectes de données comprennent l'observation des interactions au cours des réunions et en dehors du bureau, des entretiens avec les parties prenantes, et une étude de documents (documents politiques et correspondance interne et externe).

Les résultats de l'étude empirique montrent que les présomptions relatives à la technologie et à la légitimité dans les trois perspectives de surveillance ont été confirmées dans la pratique de la surveillance publique de la mobilité. Toutefois, les présomptions théoriques se sont manifestées à divers degrés. Le tableau 3 résume dans quelle mesure ces présomptions de technologie et de légitimité concernant les trois perspectives de surveillance, de contrôle, d'interaction et de précaution, ont été retrouvées dans chacune des deux études de cas. Par conséquent, il offre un aperçu des présomptions qui influencent sur la prise de décision relative aux technologies impliquées dans la surveillance publique de la mobilité.

HYPOTHESES DE TECHNOLOGIE ET LEGITIMITE	ANPR - POLICE	INNOVATION - NDW
<i>Contrôle</i>		
Contrôle à grande échelle des citoyens (présomption liée à la technologie)	Fort	Absent
Discipline des citoyens (présomption liée à technologie)	Absent	Absent
Usage de la surveillance par rapport aux citoyens (présomption liée à légitimité)	Fort	Fort
Protection de la vie privée des citoyens (présomption liée à légitimité)	Fort	Faible
<i>Interaction</i>		
Lien entre le gouvernement et les citoyens (présomption liée à technologie)	Absent	Absent
Création commune des informations (présomption liée à technologie)	Absent	Absent
Accès aux informations de surveillance (présomption liée à légitimité)	Faible	Fort
Pertinence et qualité des informations de surveillance (présomption liée à légitimité)	Faible	Fort
<i>Précaution</i>		
Identification des risques et des citoyens à risque (présomption liée à technologie)	Faible	Faible
Contrôle des risques (présomption liée à technologie)	Fort	Fort
Définition des risques et des catégories de citoyens à risque (présomption liée à légitimité)	Faible	Absent

Tableau 3: Manifestation empirique des perspectives de surveillance

Les présomptions relatives à la technologie et la légitimité dans le cadre de la surveillance publique de la mobilité, que l'on observe dans ces deux cas pratiques, ont des implications importantes dans la manière dont le gouvernement façonne sa relation avec les citoyens.

5 - Comment se façonne la relation entre le gouvernement et les citoyens selon les caractéristiques des perspectives de surveillance observées dans les pratiques politiques?

Sur la base des résultats théoriques et empiriques, j'ai tiré cinq conclusions et une conclusion générale.

1. Le lien entre les présomptions de technologie et celles de légitimité est limité.
2. Les perspectives de précaution et d'interaction sont à la hausse.
3. Le sujet mobile est de plus en plus abordé comme un risque.
4. Le gouvernement s'efforce à rendre les services imperceptibles aux et à les protéger des risques.
5. L'information fournie au coproducteur est limitée.

Conclusion générale: le citoyen mobile est perçu comme un risque

Dans les trois dimensions de la relation entre le gouvernement et les citoyens, les citoyens mobiles sont principalement considérés comme des causes potentielles de catastrophes et d'inconfort. La surveillance publique de la mobilité vise à évaluer le citoyen mobile en termes de risques pour la société. Elle permet au gouvernement d'évaluer quels sujets mobiles pourraient contrevenir aux normes et aux règles, et donc d'identifier ceux qui représentent une menace potentielle pour la société. Les clients mobiles sont également évalués en tant que facteur de risque. Le cas échéant, ils bénéficient de services imperceptibles de la part du gouvernement. Il y a aussi une perception dominante de risque en s'adressant aux coproducteurs mobiles. Ils reçoivent peu d'informations sur les activités du gouvernement liées à la surveillance publique de la mobilité parce que leur sousveillance pose un risque pour la poursuite de ces activités.

Le gouvernement ne définit pas les risques uniquement sur la base des caractéristiques de l'objet de surveillance, mais également de plus en plus à partir des données passées

et présentes concernant les mouvements des citoyens. L'analyse des caractéristiques de déplacement des citoyens pourrait mener au marquage (temporaire) de certains endroits comme zones à risque.

En abordant les citoyens et leurs déplacements comme des risques pour la société, le gouvernement interprète de manière particulière la perspective de précaution. Cette précaution vise principalement l'ensemble des citoyens mobiles qui peuvent constituer des risques, plutôt que ceux qui sont réellement à risque. La protection des citoyens mobiles contre les risques qu'ils peuvent rencontrer en route n'est pas le premier but de la surveillance publique de la mobilité. Il est en fait plutôt axé sur les dégâts que les citoyens mobiles peuvent causer à l'état et à la société.

INDEX FIGUREN EN TABELLEN

Figuur 1: Mobiliteitsgegevens.....	41
Figuur 2: Mijn locatie op drie manieren.....	45
Figuur 3: Actoren en gegevensstromen voor mobiliteitsinformatie.....	48
Figuur 4: De relatie overheid-burger.....	91
Figuur 5: Actoren en gegevensstromen ANPR Politie Nodaalstad.....	174
Figuur 6: Actoren en gegevensstromen NDW consortium 2	217
Tabel 1: Het surveillanceobject: wat beweegt er?.....	39
Tabel 2: Objectcategorieën.....	43
Tabel 3: Locatiecategorieën	45
Tabel 4: Tijds categorieën	47
Tabel 5: Surveillanceperspectieven en de relatie overheid-burger.....	118
Tabel 6: Technologie- en legitimiteitsassumpties in het controle-, interactie- en voorzorgperspectief.....	132
Tabel 7: Fictief hits report.....	160
Tabel 8: Mobiliteitsgegevens bij de toepassing van ANPR	175
Tabel 9: Technologie- en legitimiteitsassumpties in het ANPR-beleid van de Politie Nodaalstad	178
Tabel 10: Surveillanceperspectieven in het ANPR-beleid van de Politie Nodaalstad	186
Tabel 11: Implicaties van het Nodaalse ANPR-beleid voor de verhouding machthebber-onderdaan	190
Tabel 12: Implicaties van het Nodaalse ANPR-beleid voor de verhouding dienstverlener-cliënt	192
Tabel 13: Implicaties van het Nodaalse ANPR-beleid voor de verhouding democratisch instituut-citoyen	193
Tabel 14: Mobiliteitsgegevens bij verkeersinnovatie.....	221
Tabel 15: Technologie- en legitimiteitsassumpties in het innovatiebeleid van NDW	224
Tabel 16: Surveillanceperspectieven in het innovatiebeleid van NDW	233
Tabel 17: Implicaties van het innovatiebeleid van NDW voor de verhouding machthebber-onderdaan	236
Tabel 18: Implicaties van het innovatiebeleid van NDW voor de verhouding dienstverlener-cliënt	238
Tabel 19: Implicaties van het innovatiebeleid van NDW voor de verhouding democratisch instituut-citoyen	240
Tabel 20: Mobiliteitsgegevens in twee empirische casussen	246
Tabel 21: Empirische manifestatie van surveillanceperspectieven	254

Table 1: Mobility data	283
Table 2: Surveillance perspectives and the government-citizen relationship	286
Table 3: Empirical manifestation of surveillance perspectives	288

Tableau 1: Données de mobilité	293
Tableau 2: Perspectives de surveillance dans la relation gouvernement-citoyen	297
Tableau 3: Manifestation empirique des perspectives de surveillance	298

BIJLAGE I INTERVIEWGIDS CASUS ANPR-POLITIE

In u-vorm indien gepast

- **Introductie**
 - Recorder ok?
 - Uitleggen kern onderzoek
 - Mijn positie, TiU
 - Rol interviews - noodzaak ervaringen deskundigen -
 - Geheimhoudingsplicht, anonieme verwerking, vertrouwelijke behandeling
- **Positie respondent**
 - Korte loopbaangeschiedenis. Hoe lang bij politie? hoe lang bij de Politie Noodaalstad?
 - Huidige functie. Hoe lang? Voornaamste werkzaamheden. (opsporing of ook preventie?)
 - Met wie/ welke partijen werk je samen?
 - Grootste uitdaging in werk? Waarom?
- **Toepassingen ANPR**
 - Hoe lang werken met ANPR? Incidenteel/structureel (in protocol o.i.d.)? Hoe in aanraking gekomen met ANPR?
 - In hoeveel procent van je werk gebruik je ANPR-data? Is dat ongeveer gelijk aan je collega's?
 - Kan je een voorbeeld noemen van een zaak waarin je gebruik hebt gemaakt van ANPR en uitleggen hoe dat in zijn werk gaat? Begin bij begin van de zaak, een melding en dan? (contact met wie voor ANPR data? Welke data precies? Waarom? Hoe gaat zo'n aanvraag? Hoe vind je de afhandeling in de organisatie (prettig/stroef, etc.)?
 - Kan je de gewenste data altijd zonder problemen krijgen? Wanneer wel, wanneer niet? (beschikbaarheid)
 - Wat vind je van de kwaliteit van de data? (Eventueel) welke bezwaren?
 - Wat zijn de belangrijkste met ANPR behaalde resultaten tot nu toe? Kan je een concreet voorbeeld noemen?
 - Ben je betrokken bij de beleidsvorming over ANPR? Wat krijg je hiervan mee? Wordt jou om input gevraagd?

- Ethische discussie
 - Wat vind je van ANPR? Voordelen, nadelen? Wat kan er nog verbeterd worden?
 - Wat zie jij als voordelen van ANPR? Waaruit leidt je dat af? Wat zijn belangrijkste opbrengsten?
 - Kan je ook problemen of bezwaren noemen t.a.v. ANPR?
 - In hoeverre is er eensgezindheid in het korps over de toepassing van ANPR? En met externe partijen (landelijke politie, OM, gemeente). Waar is men het al over eens? Waar is men over verdeeld/ discussie over?
 - Kan je een toepassing noemen waar recentelijk discussie over is geweest binnen korps? Tot uiting in concreet overleg? Wat waren discussiepunten? Wie waren betrokkenen? Jouw rol in de discussie? Wat waren de argumenten?
 - Kan je een toepassing noemen waarvan jij denkt of hebt gedacht 'moeten we dit nu wel doen? Waarom? Heb je hier documentatie over?
- Werkwijze politie
 - In hoeverre is je werk veranderd door mogelijkheden van ANPR? Welke? In welk opzicht? In hoeverre is genoemde verandering toe te schrijven aan ANPR?
 - Wat merken burgers van ANPR? Welke burgers? Reacties tot dusver? Wat gaan ze ervan merken?
 - Hoe is communicatie tot nu toe over ANPR? Voorbeelden beschikbaar?
- Tot slot
 - Met wie zou ik nog meer moeten praten?
 - Dank! Kan ik je nog eens benaderen?

BIJLAGE II INTERVIEWGIDS CASUS INNOVATIE-NDW

In u-vorm indien gepast

- **Introductie**
 - Recorder ok?
 - Uitleggen kern onderzoek
 - Mijn positie, TiU
 - Rol interviews - noodzaak ervaringen deskundigen -
 - Anonieme verwerking, vertrouwelijke behandeling
- **Positie respondent**
 - Hoe betrokken geraakt bij aanbesteding? Gevraagd/proactief aangeboden?
 - Functie/positie in aanbestedingstraject? Doel+ voornaamste werkzaamheden.
 - Met wie/ welke partijen werk je samen/heb je overleggen?
 - Grootste uitdaging in aanbestedingstraject? Waarom?
- **Aanbesteding inwinning verkeersgegevens**
 - Wat is het precieze gebied dat wordt aanbesteed? Voor welke wegen? Welke zijn al aangesloten op NDW en welke niet?
 - Waarom vindt deze aanbesteding überhaupt plaats? Waarom nu? Waarom voor dit perceel? (EU verplichting?)
 - Aan wie worden gegevens beschikbaar gesteld?
 - Welke gegevens moeten verzameld worden en waarom?
 - Waarvoor gaan ingewonnen gegevens worden gebruikt? Welke toepassingen?
- **Waarom/waardoor innovatie**
 - Wat stelt NDW zich concreet voor bij innovatie? Waarop is deze visie gebaseerd?
 - Wat is volgens NDW het belang van innovatie?
 - In hoeverre en waarom stuurt NDW aan op innovatieve technologie?
 - Waar komt het verlangen naar innovatie vandaan? Gestimuleerd vanuit RWS/ministerie of vanuit andere hoek?
 - Hoe is innovatie überhaupt op de agenda gekomen? In hoeverre spelen eerdere experimenten met innovatieve inwintechnieken (zoals in Noord-Brabant) hierbij een rol?
 - Hoe belangrijk is het om uiteindelijk innovatie te krijgen?

- Welke voor- en nadelen zie je t.a.v. innovatieve inwintechnieken? Waar baseer je deze op? In hoeverre laat je deze meewegen in deze aanbesteding? In hoeverre bestaat hier eensgezindheid over?
 - Is er binnen NDW discussie over innovatie? Kan je een voorbeeld noemen? Weet je nog andere discussiepunten?
- Hoe innovatie bewerkstelligen
 - Hoe zeker is het dat er innovatieve inwintechnologie gebruikt gaat worden? (is er een optie dat men uiteindelijk traditionele methoden gaat gebruiken?)
 - Waarvan hangt het af of er uiteindelijk innovatieve inwintechnieken worden gebruikt of niet? Wat zijn belemmeringen? Waar liggen kansen?
 - Wat gebeurt er in de nu lopende voorbereiding van de aanbesteding om innovatie te stimuleren? Op welke manier wordt het verankerd in de aanbesteding?
- Implicaties innovatie
 - Wie gaan wat (wat gaan burgers) merken van innovatie inwinmethoden? Hoe?
 - In hoeverre gaat NDW hierover communiceren, en naar wie (naar burgers toe)?
 - Wat doet NDW als opsporingsinstanties om data komen vragen? Is deze situatie geborgd in beleidsdocumenten? Is dat in het verleden wel eens gebeurd? Hoe is dat toen verlopen?
- Tot slot
 - Met wie zou ik nog meer moeten praten?
 - Dank! Kan ik je nog eens benaderen?

OVER DE AUTEUR

Charlotte van Ooijen is geboren in Eindhoven en opgegroeid in Breda, alwaar ze in 1998 het gymnasiumdiploma behaalde. Aansluitend vertrok ze naar Groningen om aan de Rijksuniversiteit Groningen in 1999 de propaedeuse Romaanse talen en culturen en in 2003 de doctoraalstudie Communicatie- en Informatiewetenschappen (CIW) af te ronden. In de afrondende fase van CIW is tijdens onderzoeksstages bij de Gemeente Emmen en de voormalige Informatie Beheer Groep (tegenwoordig DUO) haar belangstelling voor het openbaar bestuur gewekt. Gefascineerd door de relatie tussen communicatie en beleid besloot ze aan de Radboud Universiteit in Nijmegen de Masteropleiding Bestuurskunde te volgen, die ze in 2006 afrondde met een onderzoek naar arbeidsmotivatie in de zorg.

Eind 2006 startte ze aan de Universiteit van Tilburg haar promotieonderzoek, waar dit boek de vrucht van is. Naast haar onderzoekwerkzaamheden bij het Tilburg Institute for Law, Technology, and Society droeg ze gedurende drie jaar bij aan het bestuurskunde-onderwijs van de Tilburgse School voor Politiek en Bestuur. Ze heeft meerdere papers gepresenteerd binnen de studiegroep voor informatie- en communicatietechnologie in het openbaar bestuur van de European Group for Public Administration. Ook nam ze gedurende vier jaar deel aan de Europese COST Action *Living in Surveillance Societies*. Zelfstandig en in samenwerking met collega's schreef zij (internationale) publicaties over onder meer surveillance en legitimiteit. Tijdens het laatste jaar van haar promotieonderzoek was ze werkzaam als docent en onderzoeker binnen de Capaciteitsgroep Bestuurskunde van de Erasmus Universiteit Rotterdam. De liefde voor een Fransman leidt ertoe dat Charlotte na de verdediging van haar proefschrift naar Parijs verhuist. Vanaf het najaar van 2014 is zij verbonden aan het onderzoeks- en onderwijscentrum voor bestuurskunde en politicologie (CERSA) van de Universiteit Panthéon-Assas | Paris II. Haar onderzoeksinteresses bestrijken onder meer de domeinen van openbaar bestuur, mobiliteit en technologie.